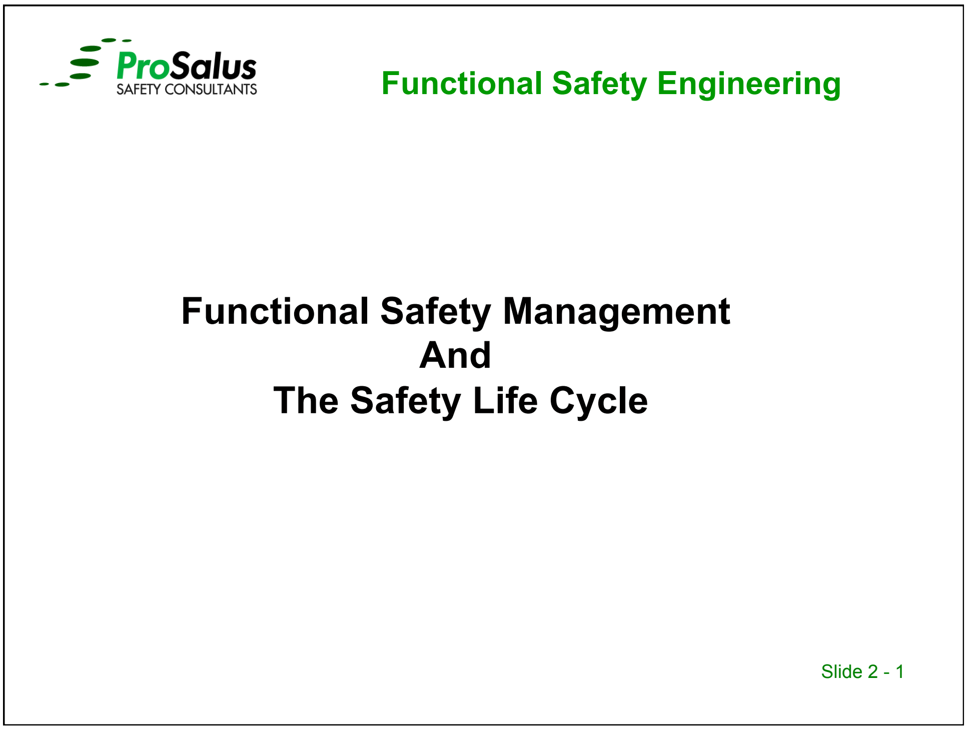
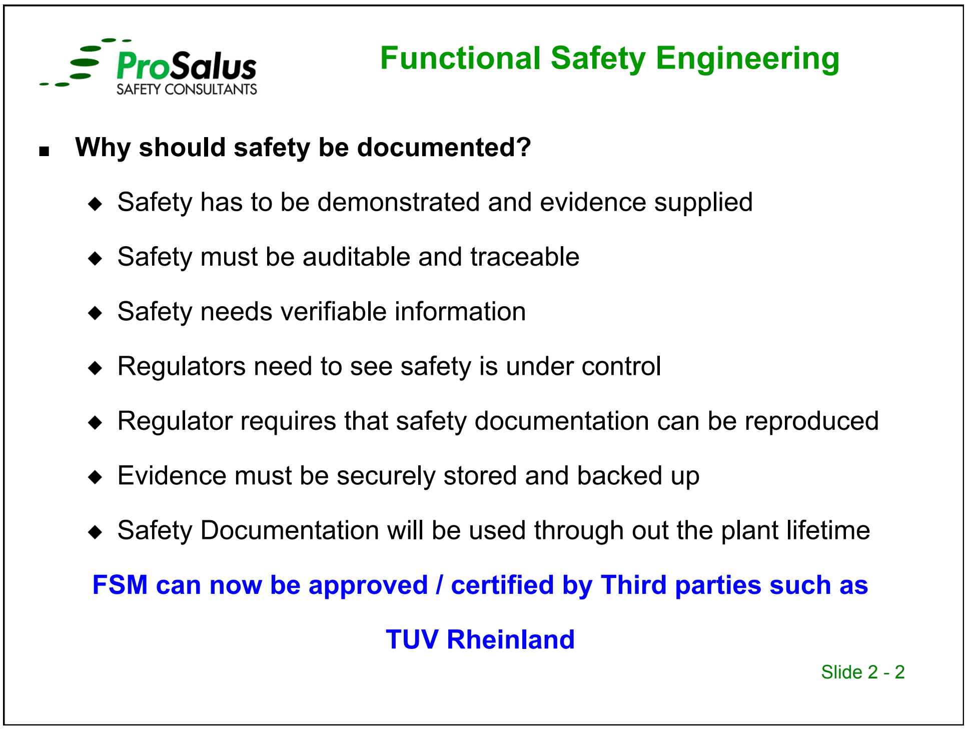


Functional Safety Engineering

Functional Safety Management
And
The Safety Life Cycle

Slide 2 - 1

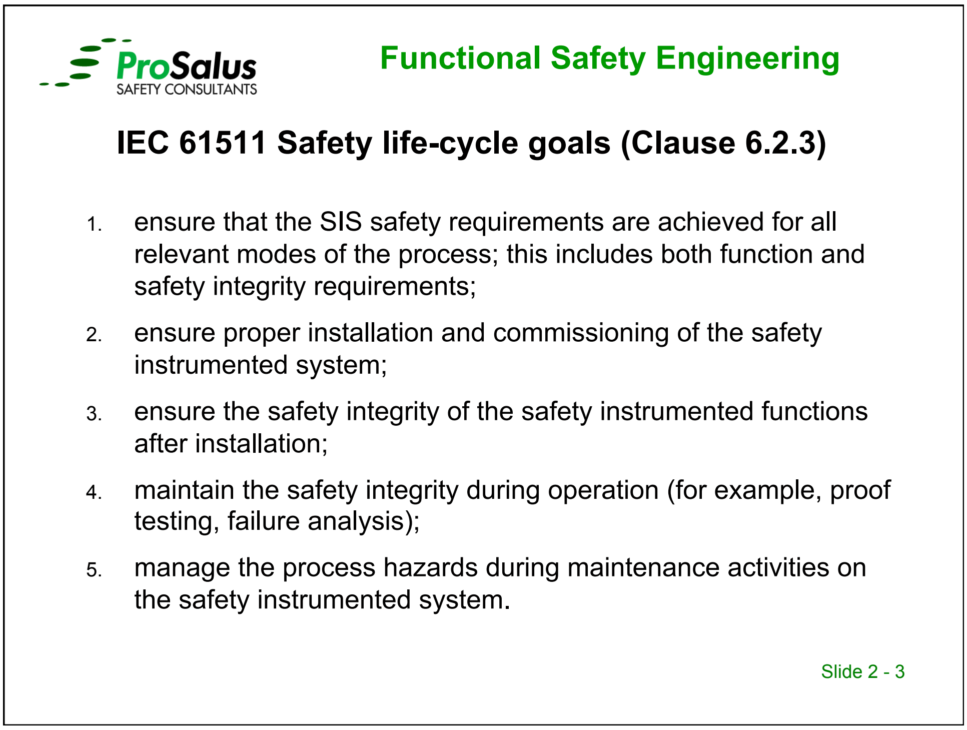


Functional Safety Engineering

- **Why should safety be documented?**
  - Safety has to be demonstrated and evidence supplied
  - Safety must be auditable and traceable
  - Safety needs verifiable information
  - Regulators need to see safety is under control
  - Regulator requires that safety documentation can be reproduced
  - Evidence must be securely stored and backed up
  - Safety Documentation will be used through out the plant lifetime

FSM can now be approved / certified by Third parties such as TUV Rheinland

Slide 2 - 2



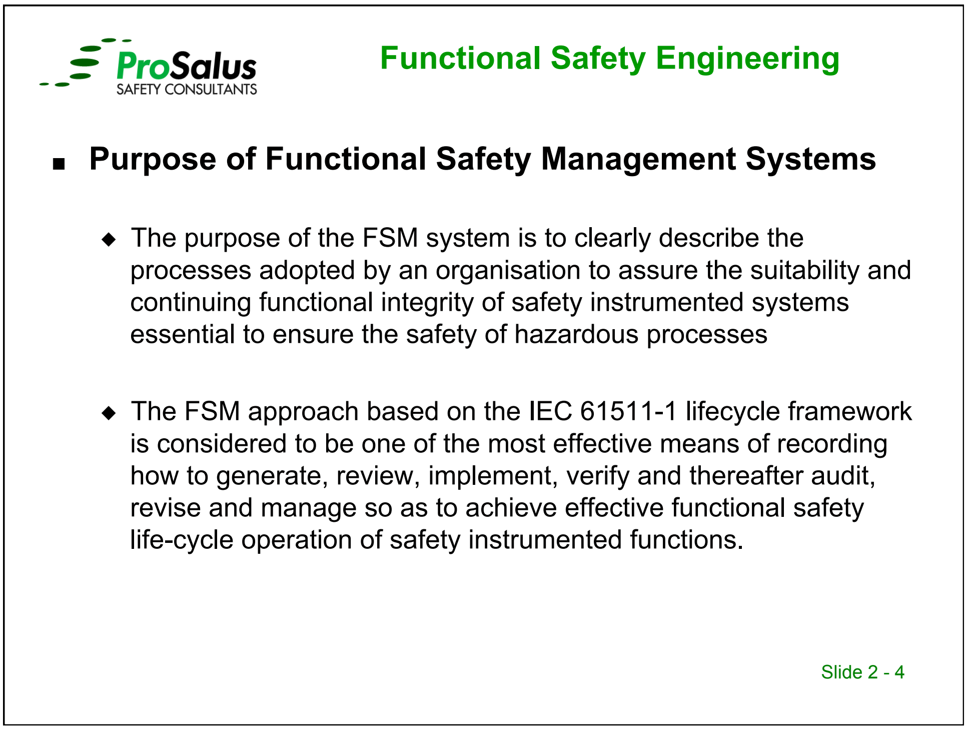
ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Safety life-cycle goals (Clause 6.2.3)

1. ensure that the SIS safety requirements are achieved for all relevant modes of the process; this includes both function and safety integrity requirements;
2. ensure proper installation and commissioning of the safety instrumented system;
3. ensure the safety integrity of the safety instrumented functions after installation;
4. maintain the safety integrity during operation (for example, proof testing, failure analysis);
5. manage the process hazards during maintenance activities on the safety instrumented system.

Slide 2 - 3

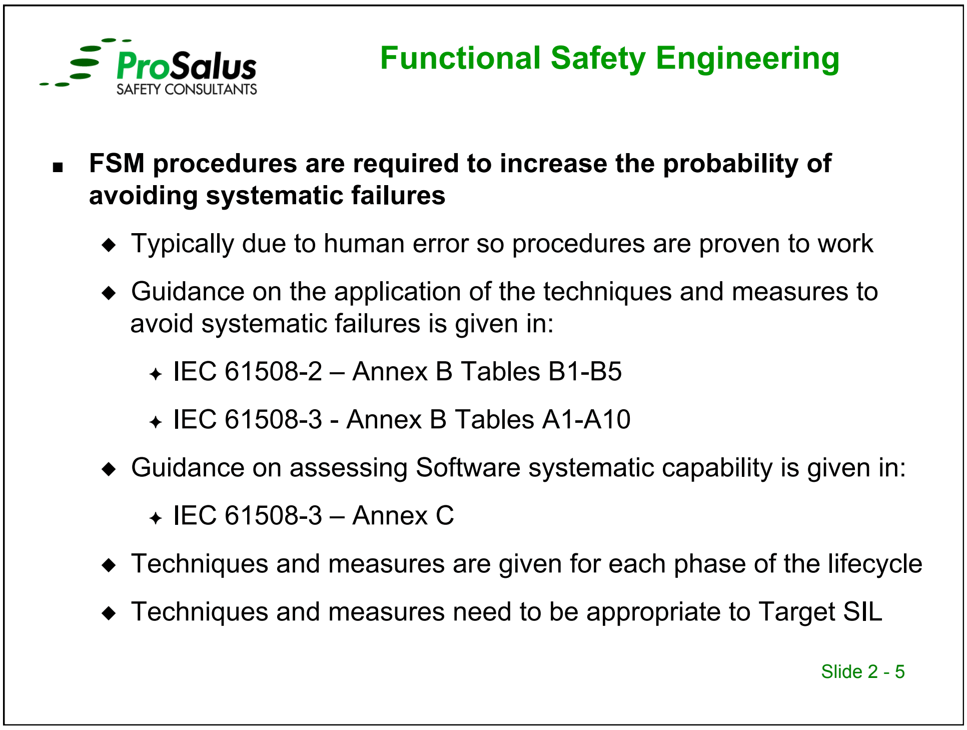


ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering

- **Purpose of Functional Safety Management Systems**
  - The purpose of the FSM system is to clearly describe the processes adopted by an organisation to assure the suitability and continuing functional integrity of safety instrumented systems essential to ensure the safety of hazardous processes
  - The FSM approach based on the IEC 61511-1 lifecycle framework is considered to be one of the most effective means of recording how to generate, review, implement, verify and thereafter audit, revise and manage so as to achieve effective functional safety life-cycle operation of safety instrumented functions.

Slide 2 - 4

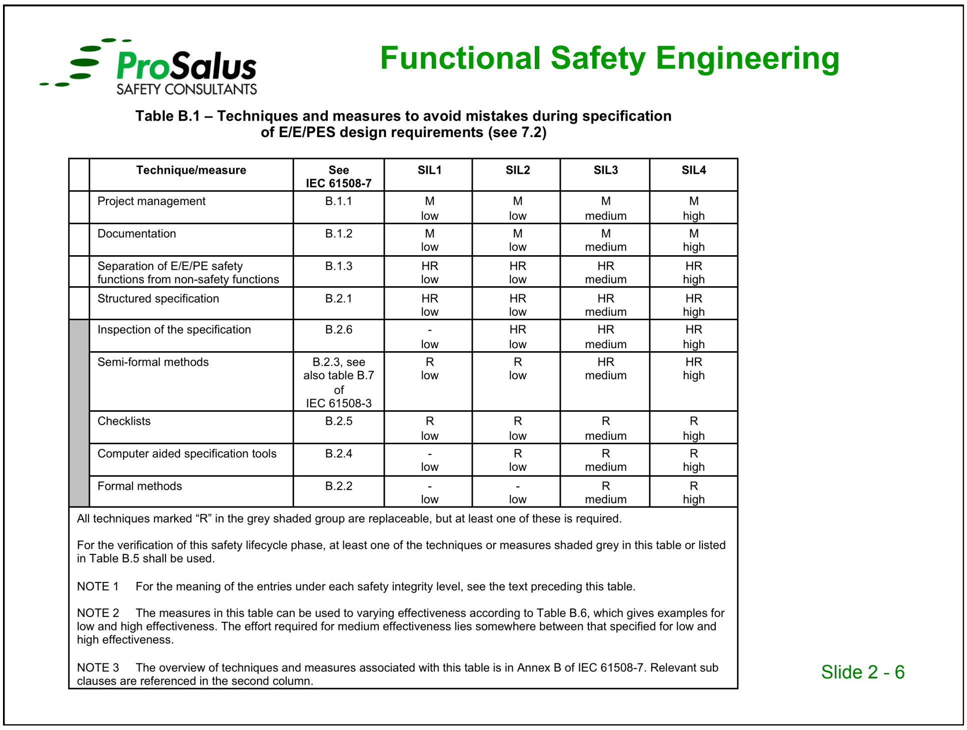


ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **FSM procedures are required to increase the probability of avoiding systematic failures**
  - ◆ Typically due to human error so procedures are proven to work
  - ◆ Guidance on the application of the techniques and measures to avoid systematic failures is given in:
    - ✦ IEC 61508-2 – Annex B Tables B1-B5
    - ✦ IEC 61508-3 - Annex B Tables A1-A10
  - ◆ Guidance on assessing Software systematic capability is given in:
    - ✦ IEC 61508-3 – Annex C
  - ◆ Techniques and measures are given for each phase of the lifecycle
  - ◆ Techniques and measures need to be appropriate to Target SIL

Slide 2 - 5



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Table B.1 – Techniques and measures to avoid mistakes during specification of E/E/PES design requirements (see 7.2)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Separation of E/E/PE safety functions from non-safety functions	B.1.3	HR low	HR low	HR medium	HR high
	Structured specification	B.2.1	HR low	HR low	HR medium	HR high
▨	Inspection of the specification	B.2.6	- low	HR low	HR medium	HR high
▨	Semi-formal methods	B.2.3, see also table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
▨	Checklists	B.2.5	R low	R low	R medium	R high
▨	Computer aided specification tools	B.2.4	- low	R low	R medium	R high
▨	Formal methods	B.2.2	- low	- low	R medium	R high

All techniques marked “R” in the grey shaded group are replaceable, but at least one of these is required.

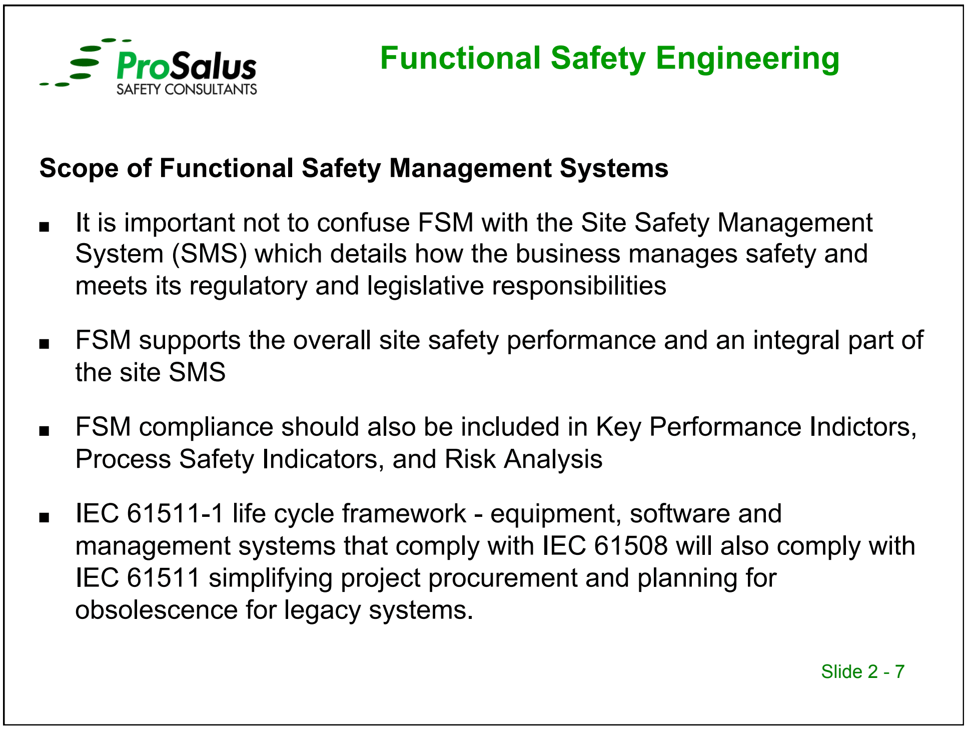
For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in Table B.5 shall be used.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding this table.

NOTE 2 The measures in this table can be used to varying effectiveness according to Table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annex B of IEC 61508-7. Relevant sub clauses are referenced in the second column.

Slide 2 - 6



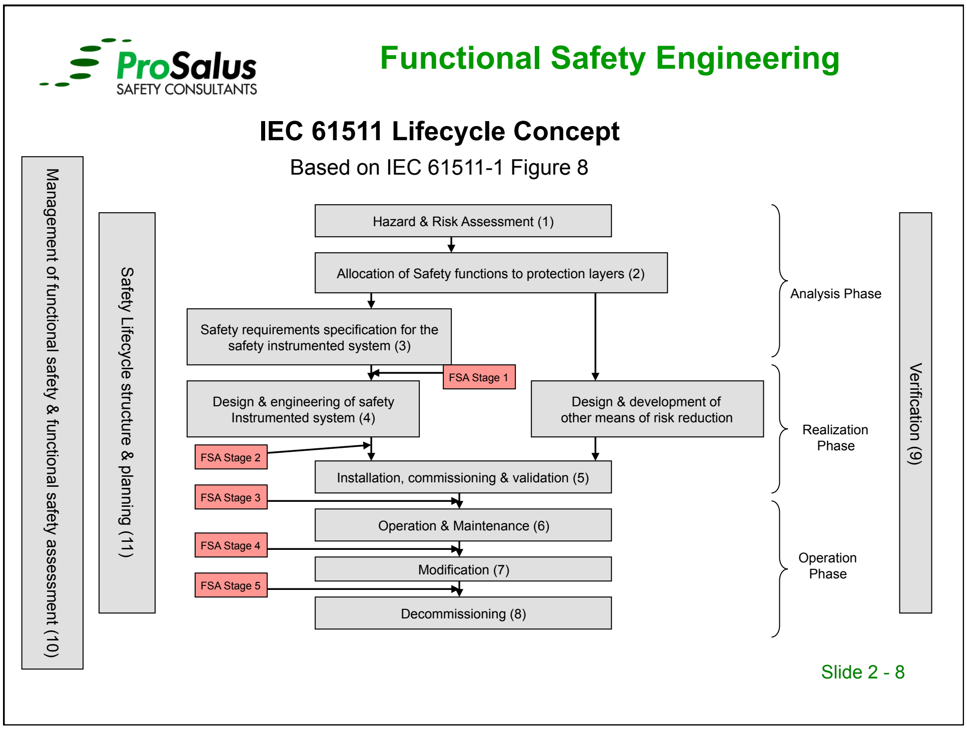
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Scope of Functional Safety Management Systems

- It is important not to confuse FSM with the Site Safety Management System (SMS) which details how the business manages safety and meets its regulatory and legislative responsibilities
- FSM supports the overall site safety performance and an integral part of the site SMS
- FSM compliance should also be included in Key Performance Indictors, Process Safety Indicators, and Risk Analysis
- IEC 61511-1 life cycle framework - equipment, software and management systems that comply with IEC 61508 will also comply with IEC 61511 simplifying project procurement and planning for obsolescence for legacy systems.

Slide 2 - 7



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Lifecycle Concept

Based on IEC 61511-1 Figure 8

Management of functional safety & functional safety assessment (10)

Safety Lifecycle structure & planning (11)

Hazard & Risk Assessment (1)

Allocation of Safety functions to protection layers (2)

Safety requirements specification for the safety instrumented system (3)

FSA Stage 1

Design & engineering of safety Instrumented system (4)

Design & development of other means of risk reduction

FSA Stage 2

Installation, commissioning & validation (5)

FSA Stage 3

Operation & Maintenance (6)

FSA Stage 4

Modification (7)

FSA Stage 5

Decommissioning (8)

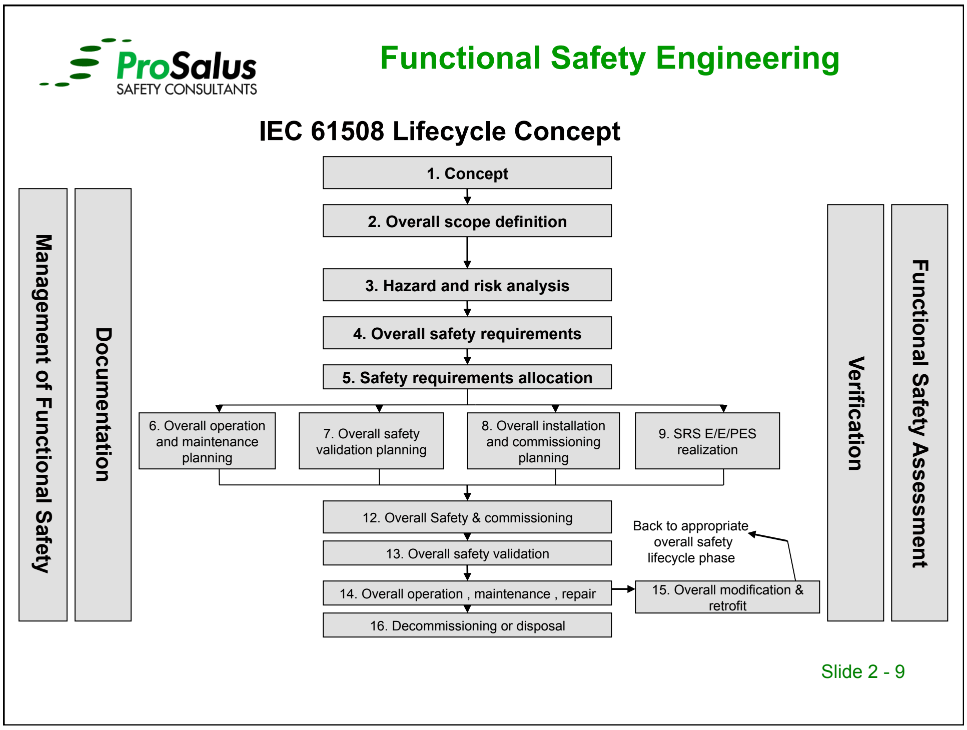
Analysis Phase

Realization Phase

Operation Phase

Verification (9)

Slide 2 - 8



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Lifecycle Concept

Management of Functional Safety

Documentation

1. Concept
2. Overall scope definition
3. Hazard and risk analysis
4. Overall safety requirements
5. Safety requirements allocation

6. Overall operation and maintenance planning

7. Overall safety validation planning

8. Overall installation and commissioning planning

9. SRS E/E/PES realization

12. Overall Safety & commissioning

13. Overall safety validation

14. Overall operation , maintenance , repair

15. Overall modification & retrofit

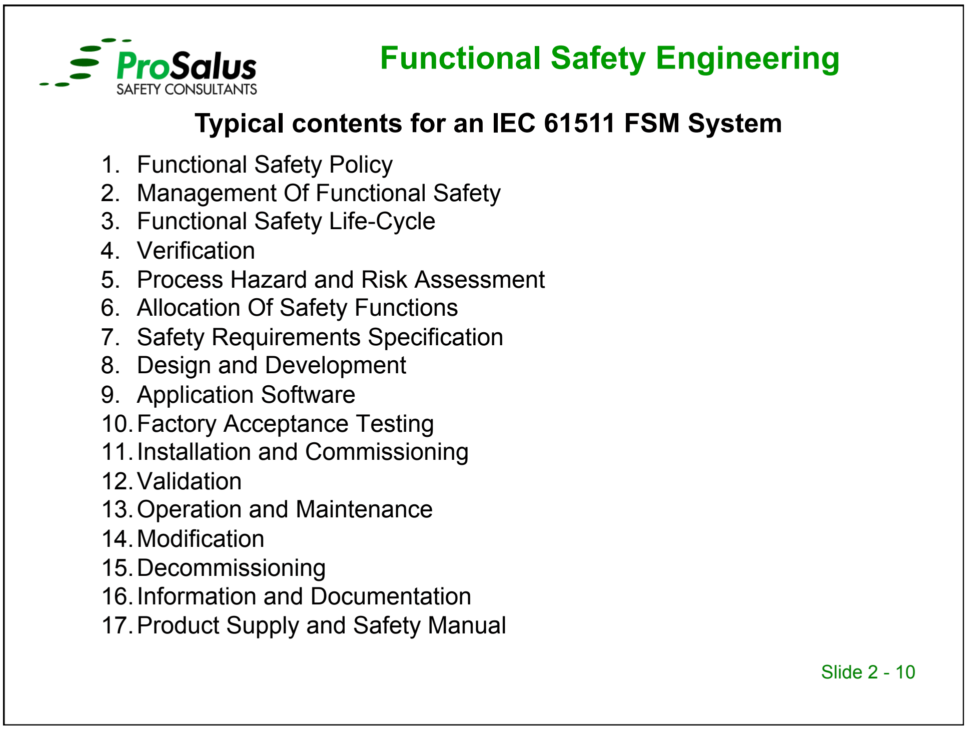
Back to appropriate overall safety lifecycle phase

16. Decommissioning or disposal

Verification

Functional Safety Assessment

Slide 2 - 9



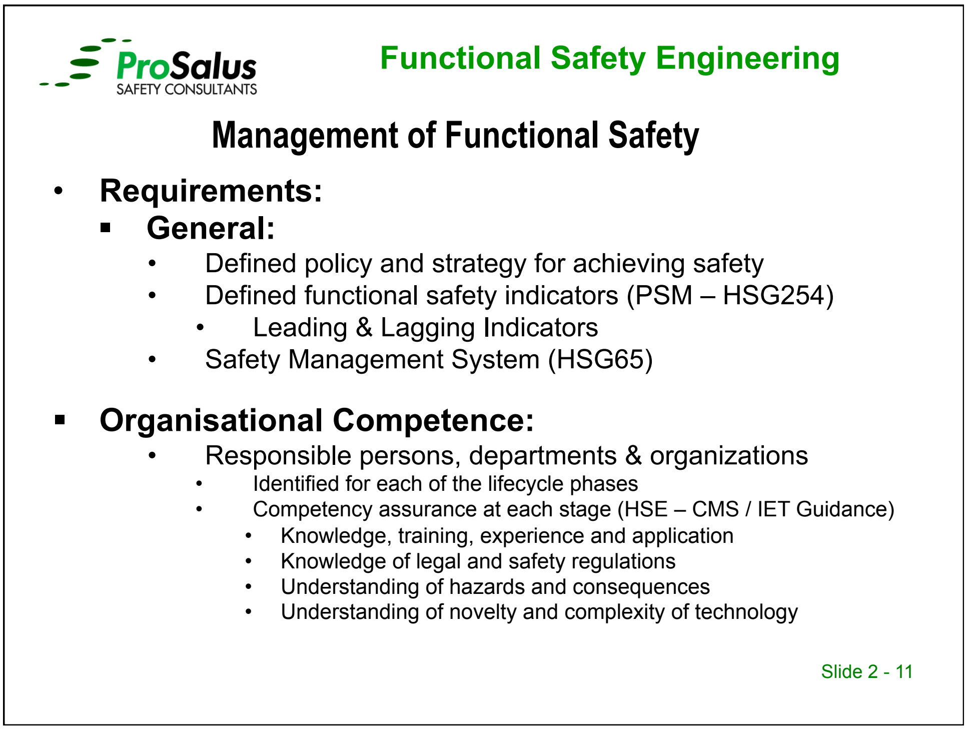
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Typical contents for an IEC 61511 FSM System

1. Functional Safety Policy
2. Management Of Functional Safety
3. Functional Safety Life-Cycle
4. Verification
5. Process Hazard and Risk Assessment
6. Allocation Of Safety Functions
7. Safety Requirements Specification
8. Design and Development
9. Application Software
10. Factory Acceptance Testing
11. Installation and Commissioning
12. Validation
13. Operation and Maintenance
14. Modification
15. Decommissioning
16. Information and Documentation
17. Product Supply and Safety Manual

Slide 2 - 10



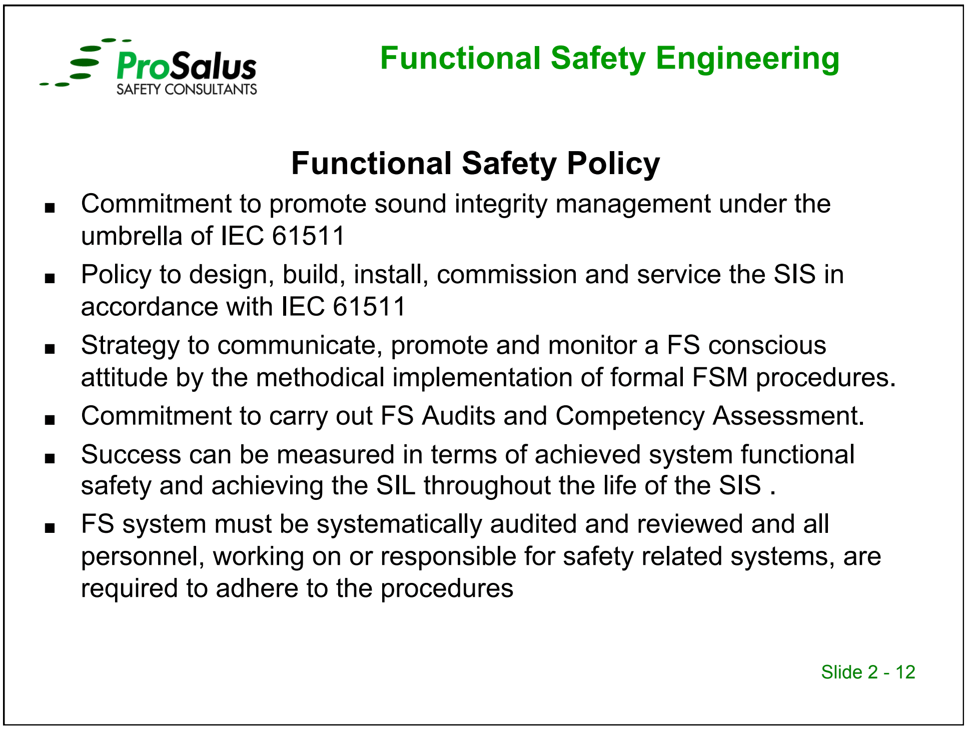
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Management of Functional Safety

- **Requirements:**
  - **General:**
    - Defined policy and strategy for achieving safety
    - Defined functional safety indicators (PSM – HSG254)
      - Leading & Lagging Indicators
    - Safety Management System (HSG65)
- **Organisational Competence:**
    - Responsible persons, departments & organizations
      - Identified for each of the lifecycle phases
      - Competency assurance at each stage (HSE – CMS / IET Guidance)
        - Knowledge, training, experience and application
        - Knowledge of legal and safety regulations
        - Understanding of hazards and consequences
        - Understanding of novelty and complexity of technology

Slide 2 - 11



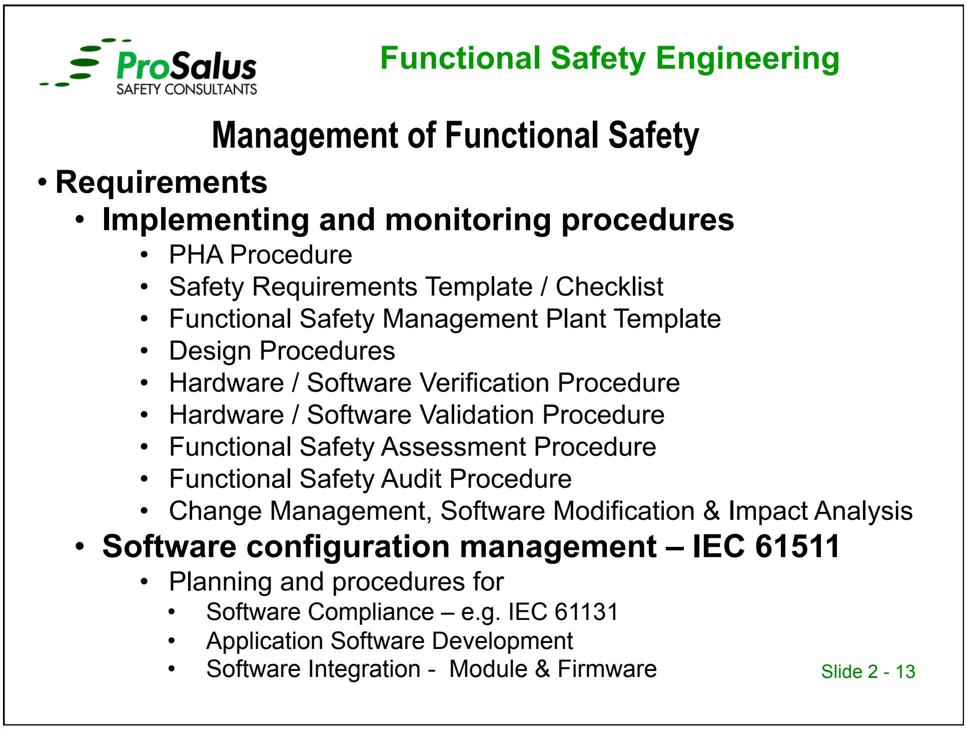
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Policy

- Commitment to promote sound integrity management under the umbrella of IEC 61511
- Policy to design, build, install, commission and service the SIS in accordance with IEC 61511
- Strategy to communicate, promote and monitor a FS conscious attitude by the methodical implementation of formal FSM procedures.
- Commitment to carry out FS Audits and Competency Assessment.
- Success can be measured in terms of achieved system functional safety and achieving the SIL throughout the life of the SIS .
- FS system must be systematically audited and reviewed and all personnel, working on or responsible for safety related systems, are required to adhere to the procedures

Slide 2 - 12



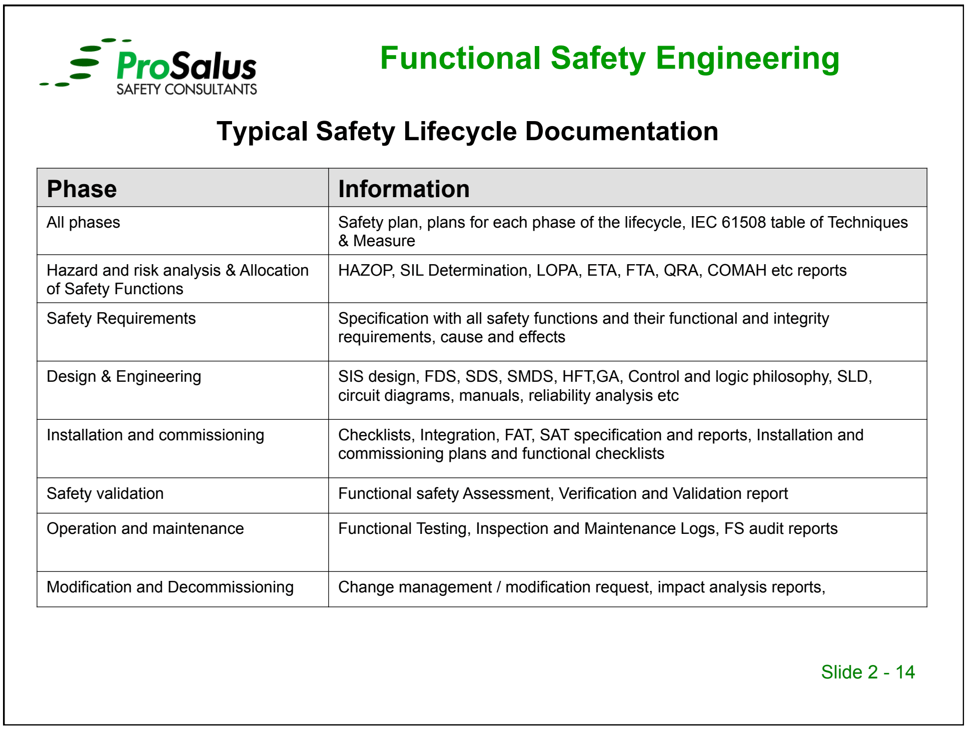
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Management of Functional Safety

- **Requirements**
  - **Implementing and monitoring procedures**
    - PHA Procedure
    - Safety Requirements Template / Checklist
    - Functional Safety Management Plant Template
    - Design Procedures
    - Hardware / Software Verification Procedure
    - Hardware / Software Validation Procedure
    - Functional Safety Assessment Procedure
    - Functional Safety Audit Procedure
    - Change Management, Software Modification & Impact Analysis
  - **Software configuration management – IEC 61511**
    - Planning and procedures for
      - Software Compliance – e.g. IEC 61131
      - Application Software Development
      - Software Integration - Module & Firmware

Slide 2 - 13



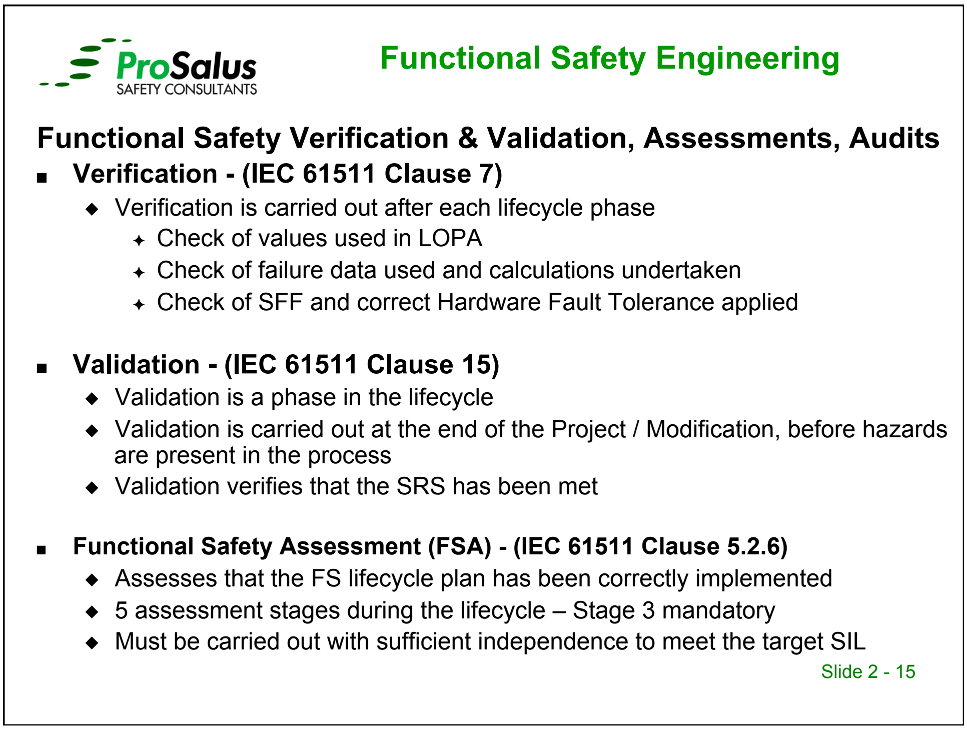
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Typical Safety Lifecycle Documentation

Phase	Information
All phases	Safety plan, plans for each phase of the lifecycle, IEC 61508 table of Techniques & Measure
Hazard and risk analysis & Allocation of Safety Functions	HAZOP, SIL Determination, LOPA, ETA, FTA, QRA, COMAH etc reports
Safety Requirements	Specification with all safety functions and their functional and integrity requirements, cause and effects
Design & Engineering	SIS design, FDS, SDS, SMDS, HFT,GA, Control and logic philosophy, SLD, circuit diagrams, manuals, reliability analysis etc
Installation and commissioning	Checklists, Integration, FAT, SAT specification and reports, Installation and commissioning plans and functional checklists
Safety validation	Functional safety Assessment, Verification and Validation report
Operation and maintenance	Functional Testing, Inspection and Maintenance Logs, FS audit reports
Modification and Decommissioning	Change management / modification request, impact analysis reports,

Slide 2 - 14



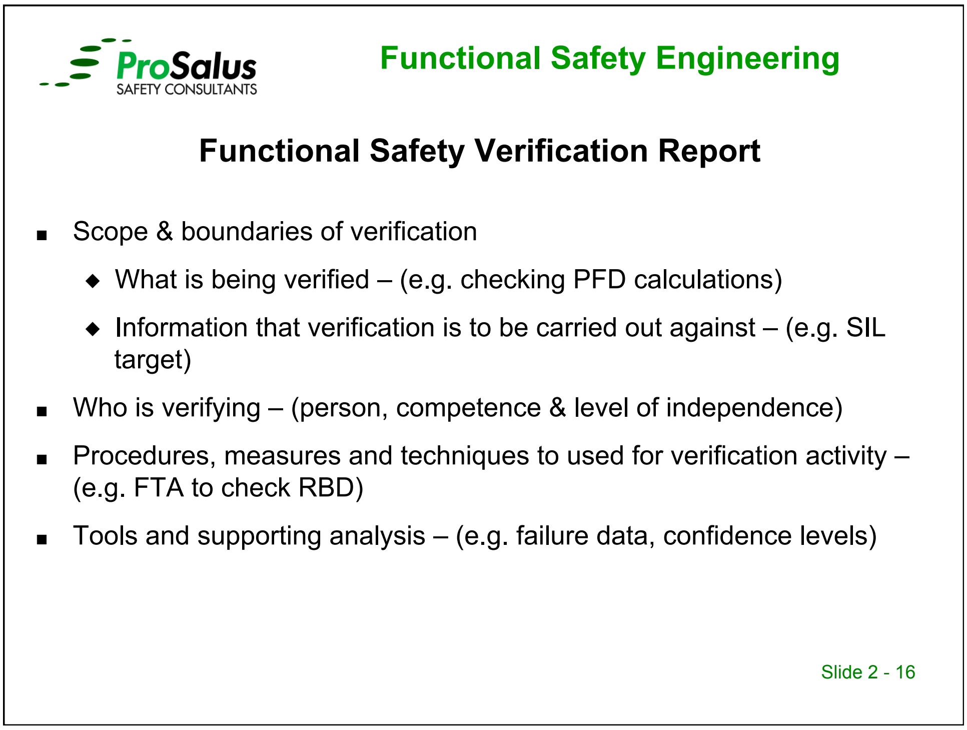
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Verification & Validation, Assessments, Audits

- **Verification - (IEC 61511 Clause 7)**
  - Verification is carried out after each lifecycle phase
    - Check of values used in LOPA
    - Check of failure data used and calculations undertaken
    - Check of SFF and correct Hardware Fault Tolerance applied
- **Validation - (IEC 61511 Clause 15)**
  - Validation is a phase in the lifecycle
  - Validation is carried out at the end of the Project / Modification, before hazards are present in the process
  - Validation verifies that the SRS has been met
- **Functional Safety Assessment (FSA) - (IEC 61511 Clause 5.2.6)**
  - Assesses that the FS lifecycle plan has been correctly implemented
  - 5 assessment stages during the lifecycle – Stage 3 mandatory
  - Must be carried out with sufficient independence to meet the target SIL

Slide 2 - 15



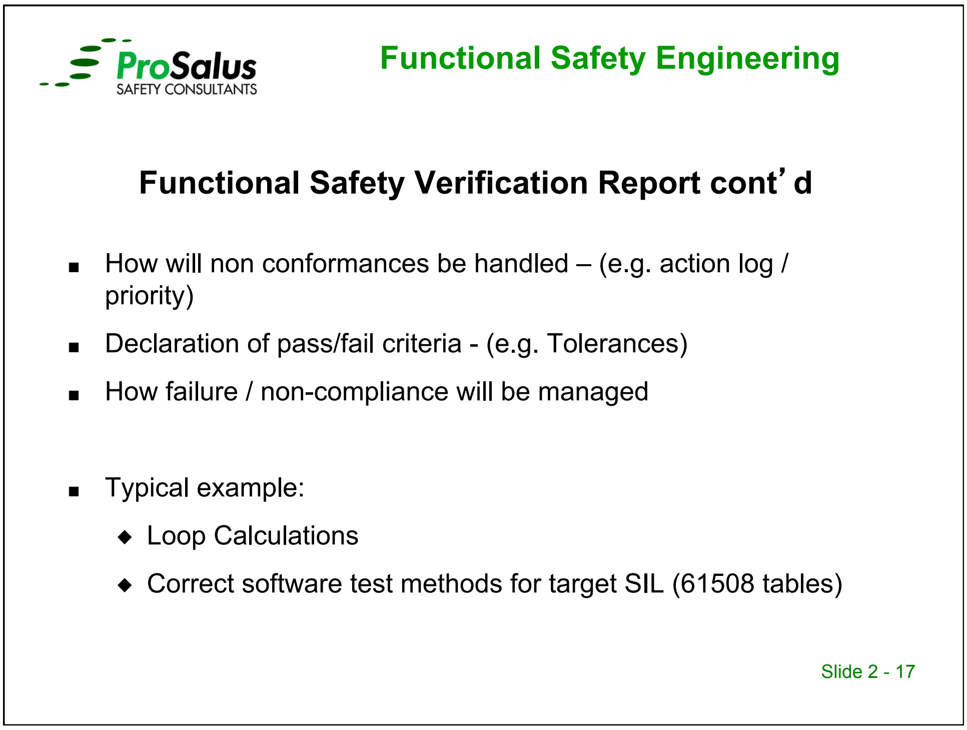
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Verification Report

- Scope & boundaries of verification
  - What is being verified – (e.g. checking PFD calculations)
  - Information that verification is to be carried out against – (e.g. SIL target)
- Who is verifying – (person, competence & level of independence)
- Procedures, measures and techniques to used for verification activity – (e.g. FTA to check RBD)
- Tools and supporting analysis – (e.g. failure data, confidence levels)

Slide 2 - 16



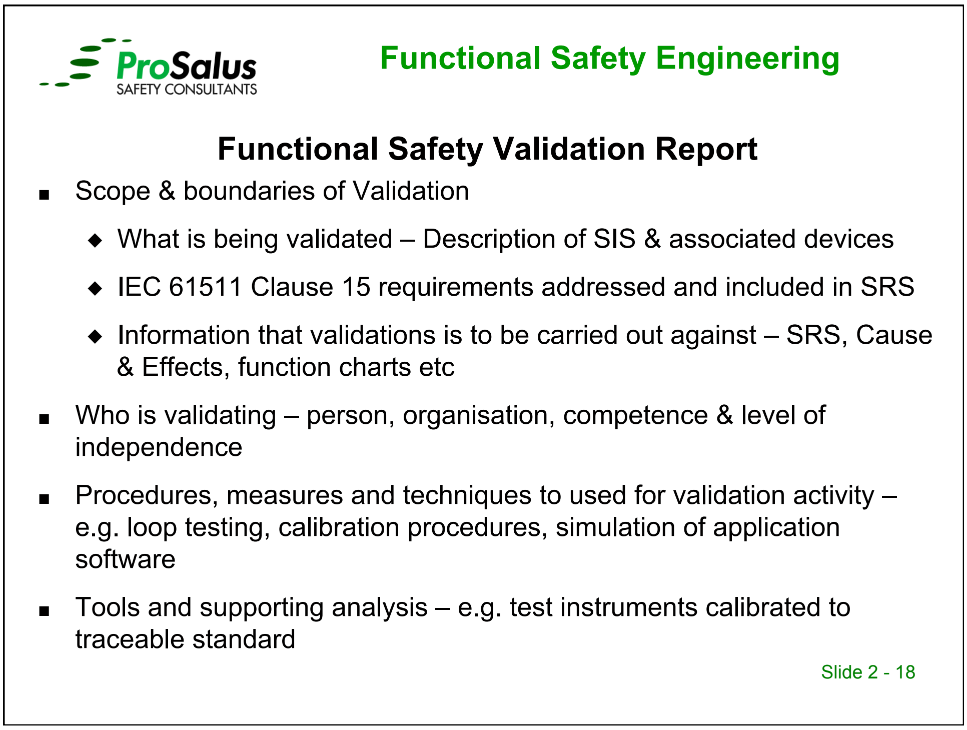
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Verification Report cont’d

- How will non conformances be handled – (e.g. action log / priority)
- Declaration of pass/fail criteria - (e.g. Tolerances)
- How failure / non-compliance will be managed
- Typical example:
  - Loop Calculations
  - Correct software test methods for target SIL (61508 tables)

Slide 2 - 17



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Validation Report

- Scope & boundaries of Validation
  - What is being validated – Description of SIS & associated devices
  - IEC 61511 Clause 15 requirements addressed and included in SRS
  - Information that validations is to be carried out against – SRS, Cause & Effects, function charts etc
- Who is validating – person, organisation, competence & level of independence
- Procedures, measures and techniques to used for validation activity – e.g. loop testing, calibration procedures, simulation of application software
- Tools and supporting analysis – e.g. test instruments calibrated to traceable standard

Slide 2 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety (SIL) Validation Report cont’d

- How will non conformances be handled – e.g. action log / priority
- Tools & techniques appropriate for Target SIL
  - IEC 61508-2 – Table B.5
  - IEC 61508-3 – Table A.7
- Declaration of pass/fail criteria - e.g. SRS not met, logic not as per Cause & Effect. Timing requirements not met
- Typical example:
  - Completed Loop test procedure
  - Correct software test methods for target SIL (61508 tables)

Slide 2 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

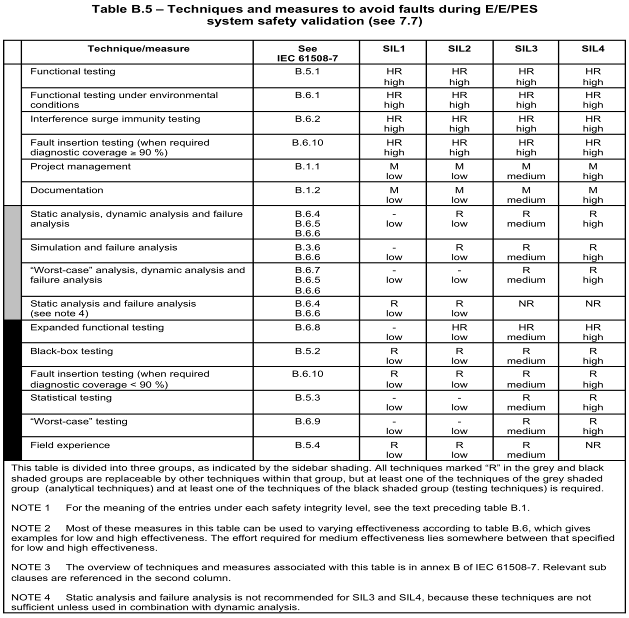


Table B.5 – Techniques and measures to avoid faults during E/E/PES system safety validation (see 7.7)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Functional testing	B.5.1	HR high	HR high	HR high	HR high
	Functional testing under environmental conditions	B.6.1	HR high	HR high	HR high	HR high
	Interference surge immunity testing	B.6.2	HR high	HR high	HR high	HR high
	Fault insertion testing (when required diagnostic coverage ≥ 90 %)	B.6.10	HR high	HR high	HR high	HR high
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
░	Static analysis, dynamic analysis and failure analysis	B.6.4 B.6.5 B.6.6	- low	R low	R medium	R high
░	Simulation and failure analysis	B.3.6 B.6.6	- low	R low	R medium	R high
░	“Worst-case” analysis, dynamic analysis and failure analysis	B.6.7 B.6.5 B.6.6	- low	- low	R medium	R high
░	Static analysis and failure analysis (see note 4)	B.6.4 B.6.6	R low	R low	NR	NR
■	Expanded functional testing	B.6.8	- low	HR low	HR medium	HR high
■	Black-box testing	B.5.2	R low	R low	R medium	R high
■	Fault insertion testing (when required diagnostic coverage < 90 %)	B.6.10	R low	R low	R medium	R high
■	Statistical testing	B.5.3	- low	- low	R medium	R high
■	“Worst-case” testing	B.6.9	- low	- low	R medium	R high
■	Field experience	B.5.4	R low	R low	R medium	NR

This table is divided into three groups, as indicated by the sidebar shading. All techniques marked “R” in the grey and black shaded groups are replaceable by other techniques within that group, but at least one of the techniques of the grey shaded group (analytical techniques) and at least one of the techniques of the black shaded group (testing techniques) is required.

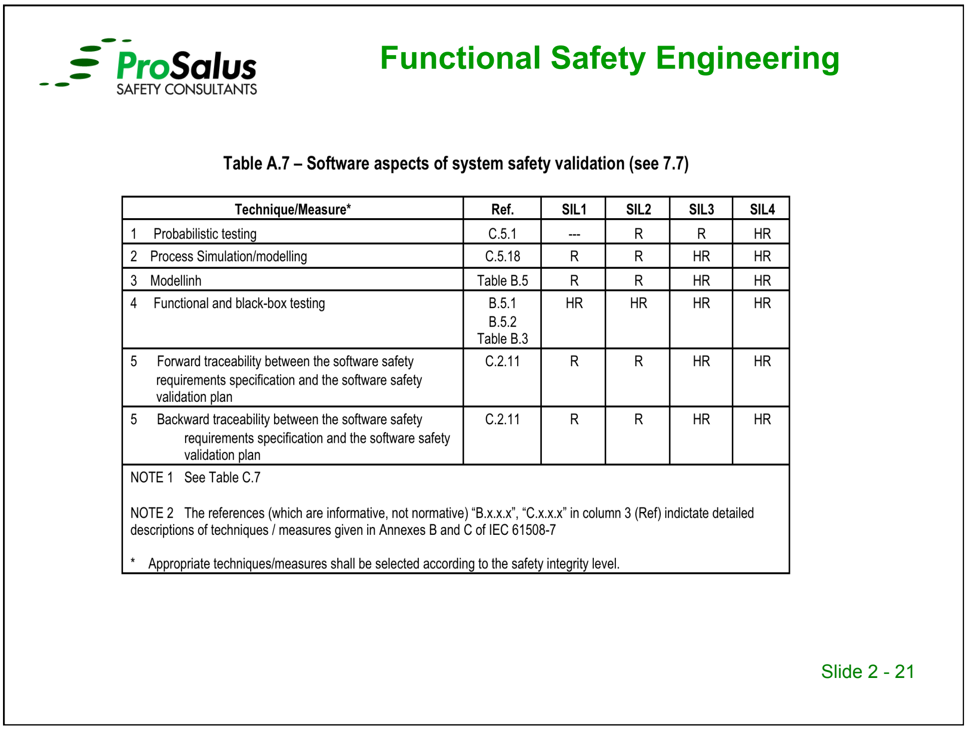
NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annex B of IEC 61508-7. Relevant sub clauses are referenced in the second column.

NOTE 4 Static analysis and failure analysis is not recommended for SIL3 and SIL4, because these techniques are not sufficient unless used in combination with dynamic analysis.

Slide 2 - 20



Functional Safety Engineering

ProSalus SAFETY CONSULTANTS

Table A.7 – Software aspects of system safety validation (see 7.7)

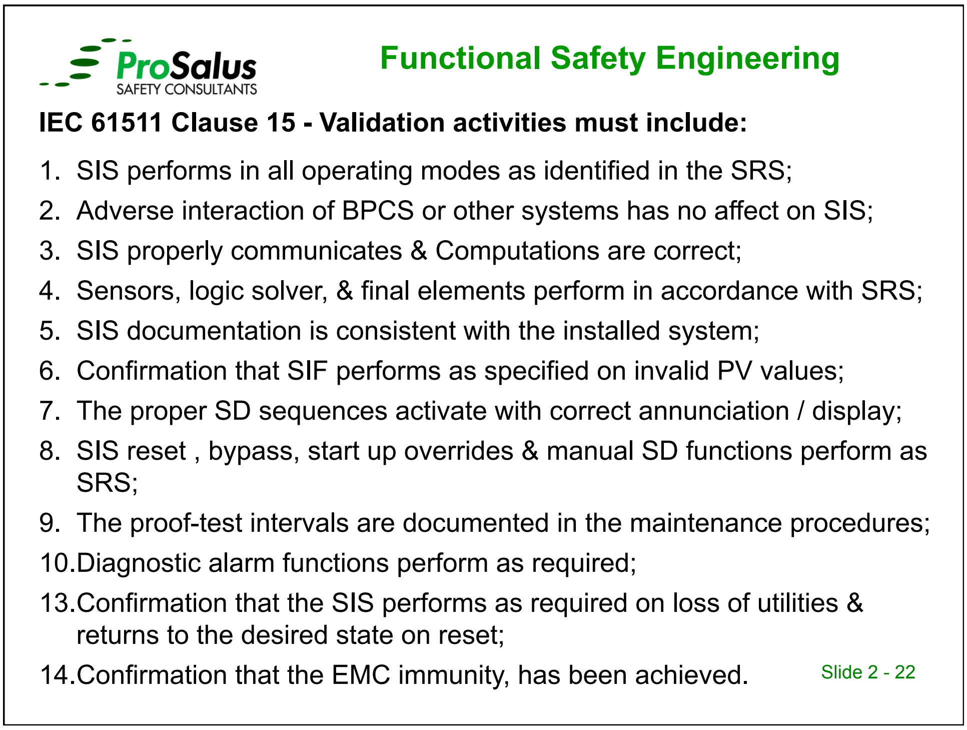
Technique/Measure*	Ref.	SIL1	SIL2	SIL3	SIL4
1 Probabilistic testing	C.5.1	---	R	R	HR
2 Process Simulation/modelling	C.5.18	R	R	HR	HR
3 Modellinh	Table B.5	R	R	HR	HR
4 Functional and black-box testing	B.5.1 B.5.2 Table B.3	HR	HR	HR	HR
5 Forward traceability between the software safety requirements specification and the software safety validation plan	C.2.11	R	R	HR	HR
5 Backward traceability between the software safety requirements specification and the software safety validation plan	C.2.11	R	R	HR	HR

NOTE 1 See Table C.7

NOTE 2 The references (which are informative, not normative) "B.x.x.x", "C.x.x.x" in column 3 (Ref) indictate detailed descriptions of techniques / measures given in Annexes B and C of IEC 61508-7

* Appropriate techniques/measures shall be selected according to the safety integrity level.

Slide 2 - 21



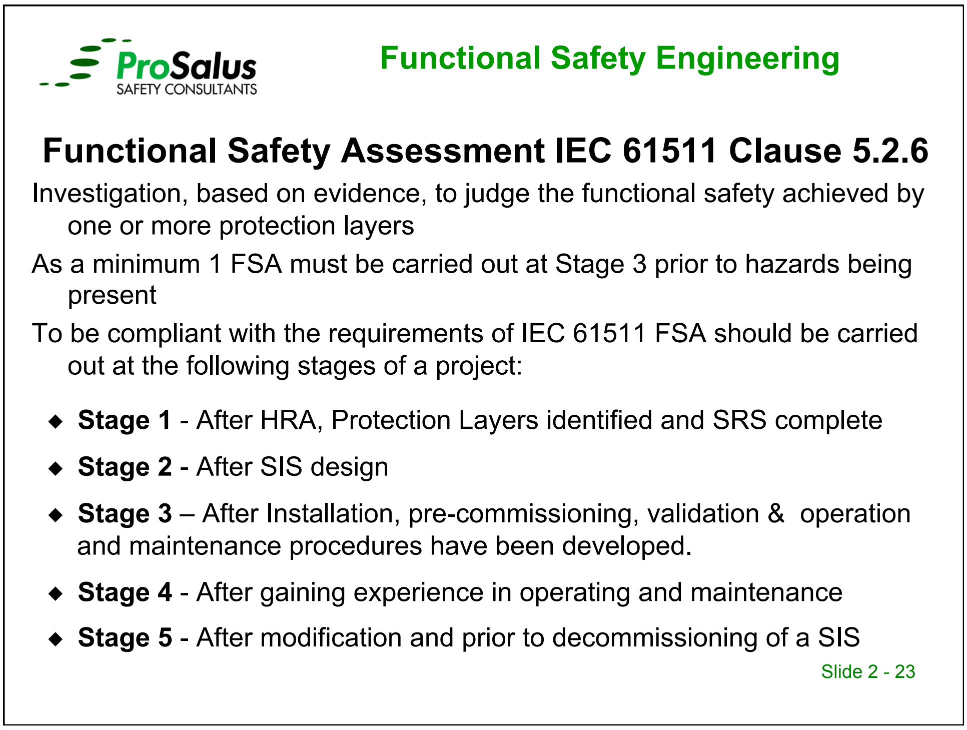
Functional Safety Engineering

ProSalus SAFETY CONSULTANTS

IEC 61511 Clause 15 - Validation activities must include:

1. SIS performs in all operating modes as identified in the SRS;
2. Adverse interaction of BPCS or other systems has no affect on SIS;
3. SIS properly communicates & Computations are correct;
4. Sensors, logic solver, & final elements perform in accordance with SRS;
5. SIS documentation is consistent with the installed system;
6. Confirmation that SIF performs as specified on invalid PV values;
7. The proper SD sequences activate with correct annunciation / display;
8. SIS reset , bypass, start up overrides & manual SD functions perform as SRS;
9. The proof-test intervals are documented in the maintenance procedures;
10. Diagnostic alarm functions perform as required;
13. Confirmation that the SIS performs as required on loss of utilities & returns to the desired state on reset;
14. Confirmation that the EMC immunity, has been achieved.

Slide 2 - 22



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Assessment IEC 61511 Clause 5.2.6

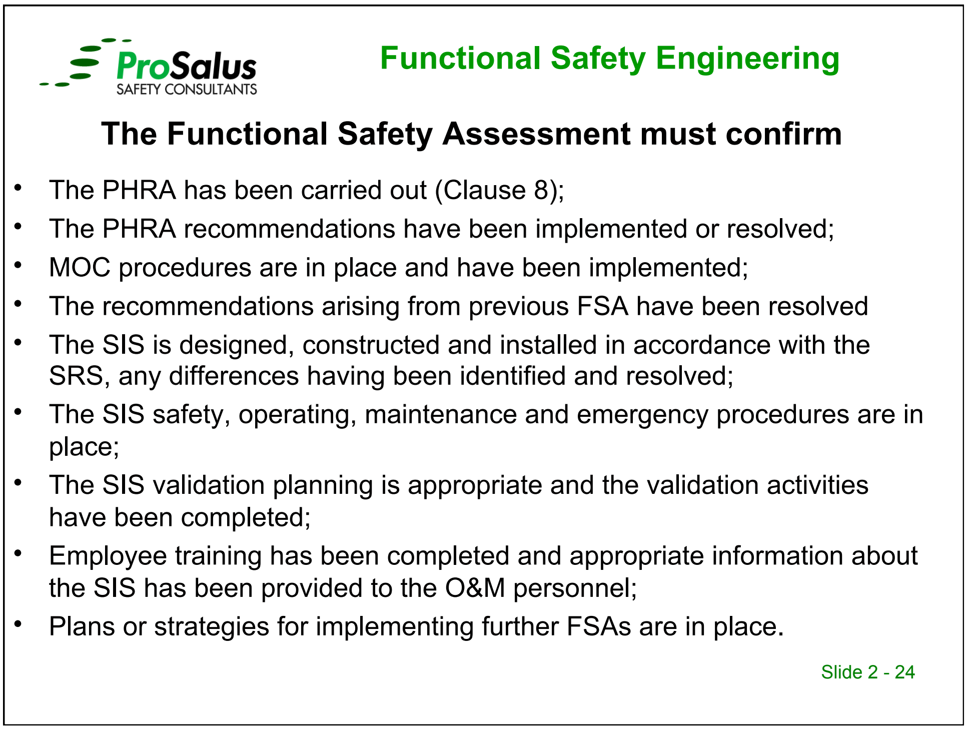
Investigation, based on evidence, to judge the functional safety achieved by one or more protection layers

As a minimum 1 FSA must be carried out at Stage 3 prior to hazards being present

To be compliant with the requirements of IEC 61511 FSA should be carried out at the following stages of a project:

- **Stage 1** - After HRA, Protection Layers identified and SRS complete
- **Stage 2** - After SIS design
- **Stage 3** – After Installation, pre-commissioning, validation & operation and maintenance procedures have been developed.
- **Stage 4** - After gaining experience in operating and maintenance
- **Stage 5** - After modification and prior to decommissioning of a SIS

Slide 2 - 23



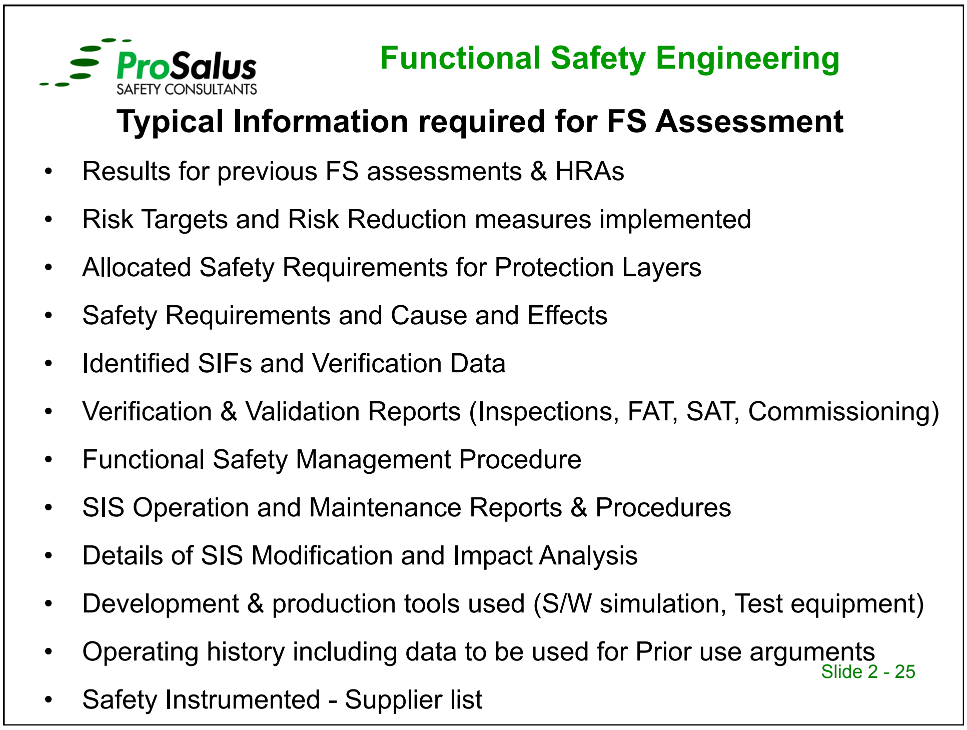
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Functional Safety Assessment must confirm

- The PHRA has been carried out (Clause 8);
- The PHRA recommendations have been implemented or resolved;
- MOC procedures are in place and have been implemented;
- The recommendations arising from previous FSA have been resolved
- The SIS is designed, constructed and installed in accordance with the SRS, any differences having been identified and resolved;
- The SIS safety, operating, maintenance and emergency procedures are in place;
- The SIS validation planning is appropriate and the validation activities have been completed;
- Employee training has been completed and appropriate information about the SIS has been provided to the O&M personnel;
- Plans or strategies for implementing further FSAs are in place.

Slide 2 - 24



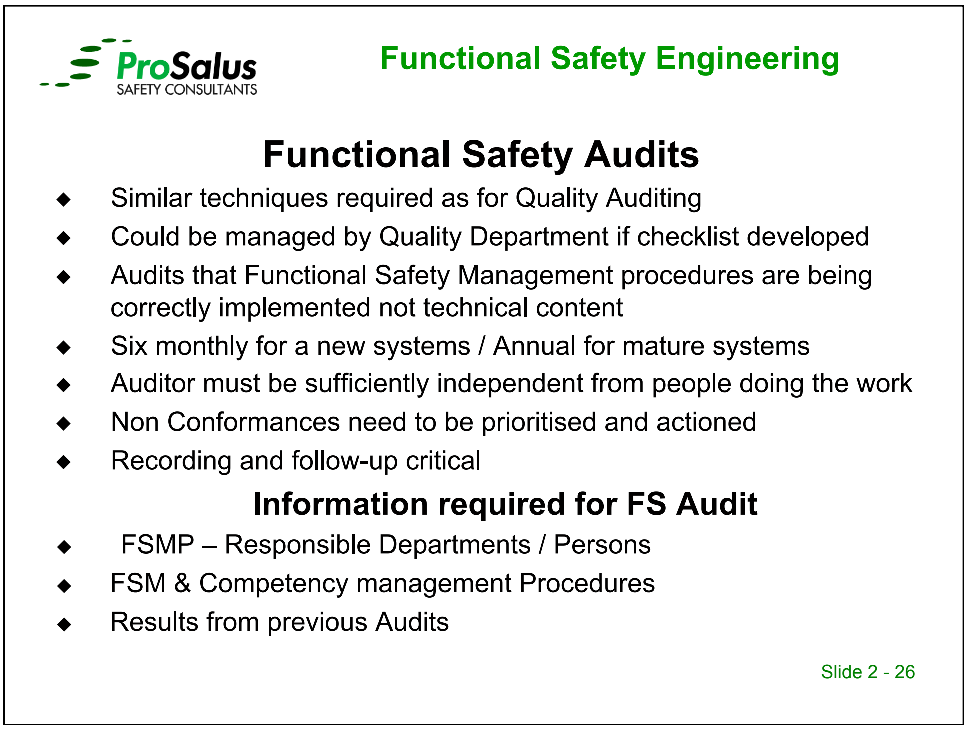
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Typical Information required for FS Assessment

- Results for previous FS assessments & HRAs
- Risk Targets and Risk Reduction measures implemented
- Allocated Safety Requirements for Protection Layers
- Safety Requirements and Cause and Effects
- Identified SIFs and Verification Data
- Verification & Validation Reports (Inspections, FAT, SAT, Commissioning)
- Functional Safety Management Procedure
- SIS Operation and Maintenance Reports & Procedures
- Details of SIS Modification and Impact Analysis
- Development & production tools used (S/W simulation, Test equipment)
- Operating history including data to be used for Prior use arguments
- Safety Instrumented - Supplier list

Slide 2 - 25



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

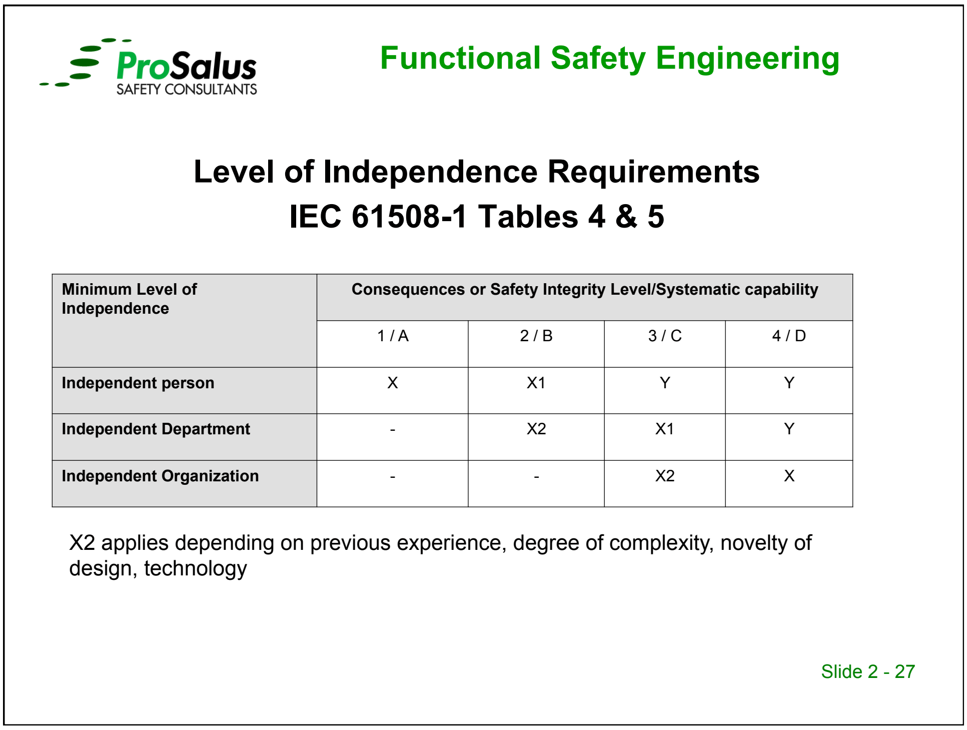
Functional Safety Audits

- Similar techniques required as for Quality Auditing
- Could be managed by Quality Department if checklist developed
- Audits that Functional Safety Management procedures are being correctly implemented not technical content
- Six monthly for a new systems / Annual for mature systems
- Auditor must be sufficiently independent from people doing the work
- Non Conformances need to be prioritised and actioned
- Recording and follow-up critical

Information required for FS Audit

- FSMP – Responsible Departments / Persons
- FSM & Competency management Procedures
- Results from previous Audits

Slide 2 - 26



ProSalus SAFETY CONSULTANTS

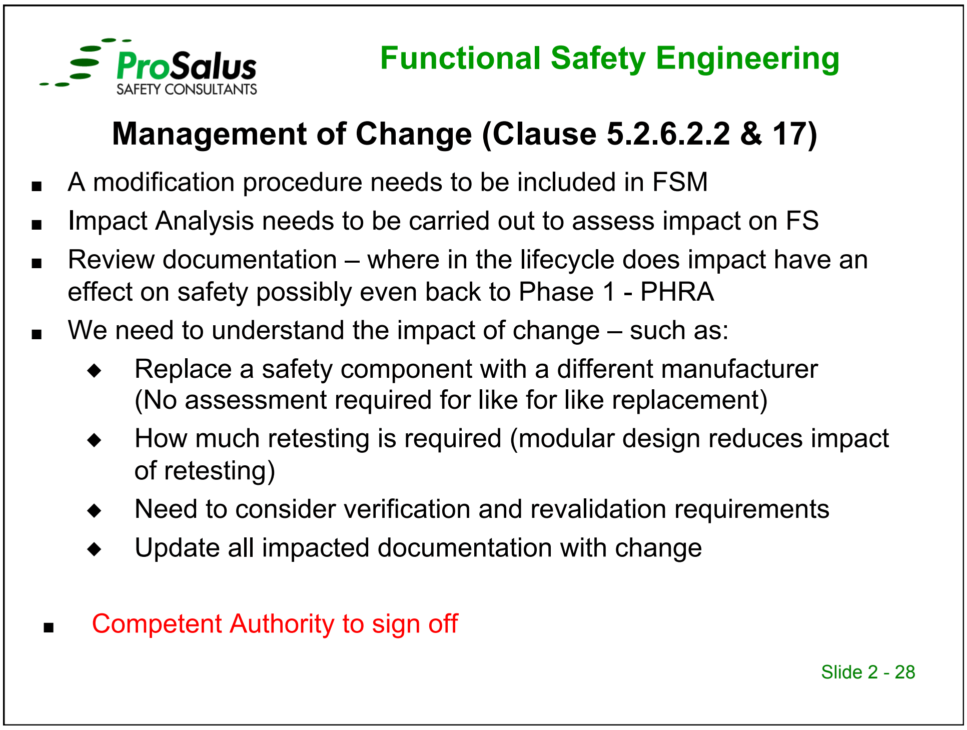
Functional Safety Engineering

Level of Independence Requirements IEC 61508-1 Tables 4 & 5

Minimum Level of Independence	Consequences or Safety Integrity Level/Systematic capability			
	1 / A	2 / B	3 / C	4 / D
Independent person	X	X1	Y	Y
Independent Department	-	X2	X1	Y
Independent Organization	-	-	X2	X

X2 applies depending on previous experience, degree of complexity, novelty of design, technology

Slide 2 - 27



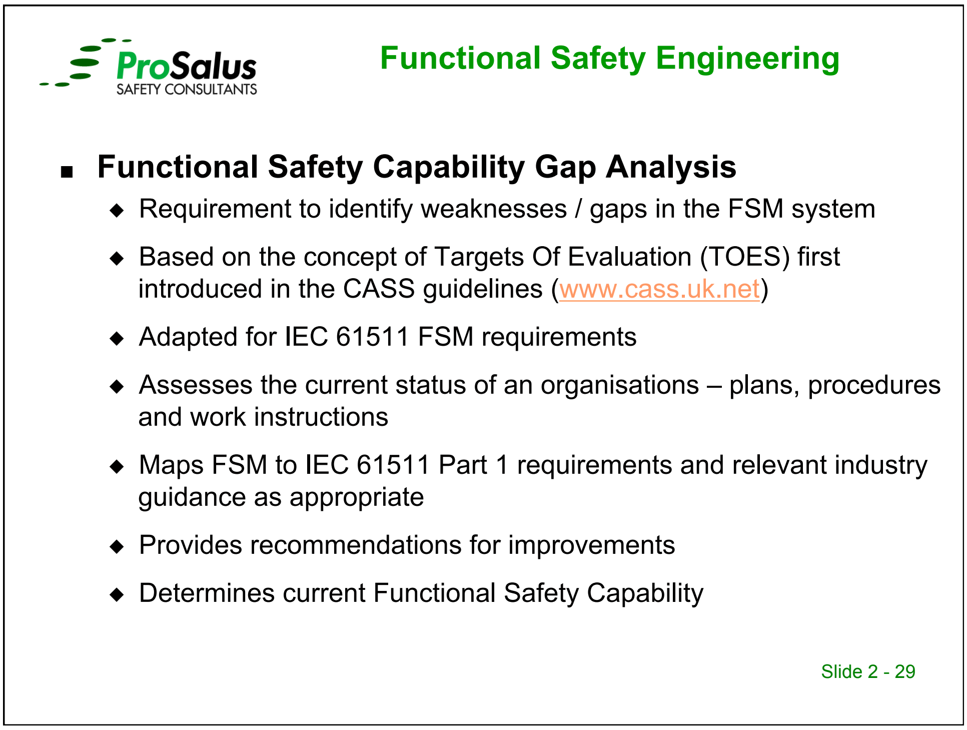
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Management of Change (Clause 5.2.6.2.2 & 17)

- A modification procedure needs to be included in FSM
- Impact Analysis needs to be carried out to assess impact on FS
- Review documentation – where in the lifecycle does impact have an effect on safety possibly even back to Phase 1 - PHRA
- We need to understand the impact of change – such as:
  - Replace a safety component with a different manufacturer (No assessment required for like for like replacement)
  - How much retesting is required (modular design reduces impact of retesting)
  - Need to consider verification and revalidation requirements
  - Update all impacted documentation with change
- Competent Authority to sign off

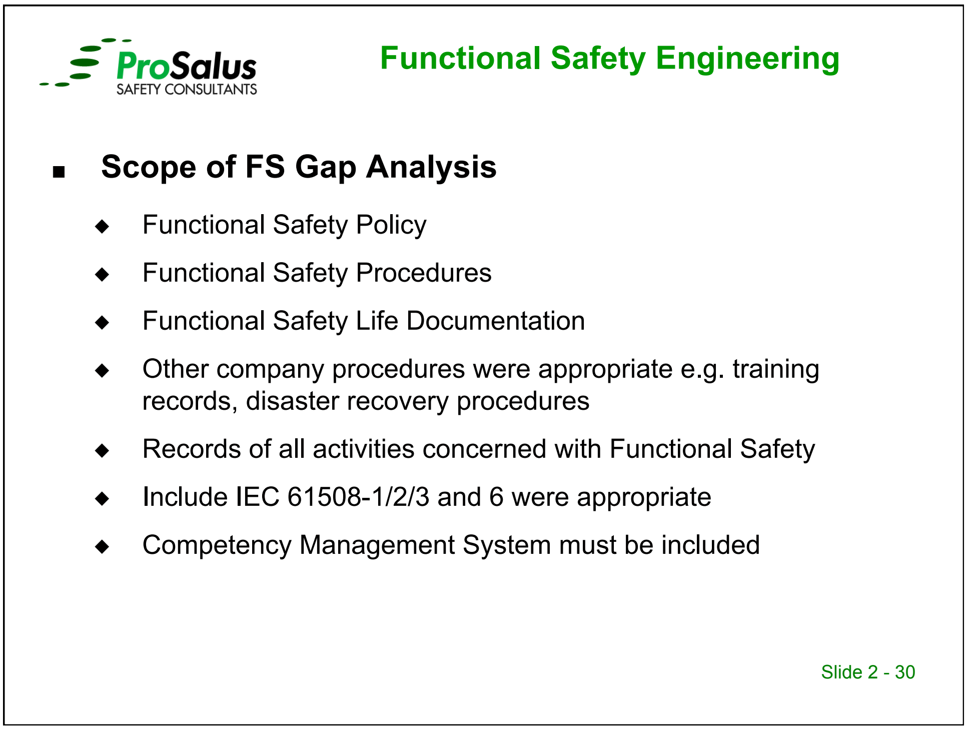
Slide 2 - 28



Functional Safety Engineering

- **Functional Safety Capability Gap Analysis**
  - Requirement to identify weaknesses / gaps in the FSM system
  - Based on the concept of Targets Of Evaluation (TOES) first introduced in the CASS guidelines (www.cass.uk.net)
  - Adapted for IEC 61511 FSM requirements
  - Assesses the current status of an organisations – plans, procedures and work instructions
  - Maps FSM to IEC 61511 Part 1 requirements and relevant industry guidance as appropriate
  - Provides recommendations for improvements
  - Determines current Functional Safety Capability

Slide 2 - 29



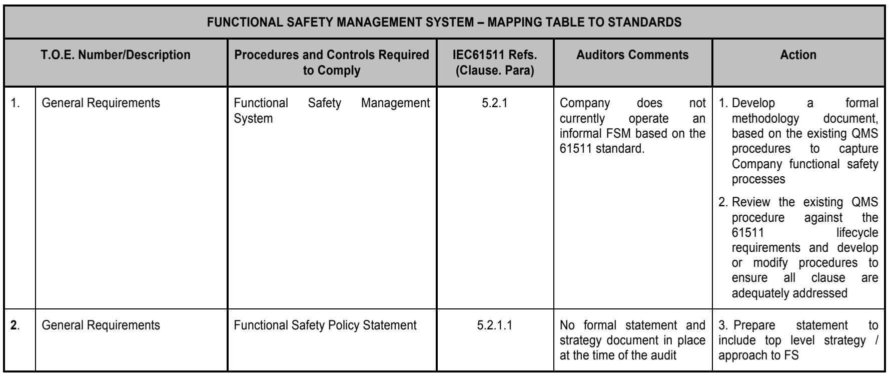
Functional Safety Engineering

- **Scope of FS Gap Analysis**
  - Functional Safety Policy
  - Functional Safety Procedures
  - Functional Safety Life Documentation
  - Other company procedures were appropriate e.g. training records, disaster recovery procedures
  - Records of all activities concerned with Functional Safety
  - Include IEC 61508-1/2/3 and 6 were appropriate
  - Competency Management System must be included

Slide 2 - 30

ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering



FUNCTIONAL SAFETY MANAGEMENT SYSTEM – MAPPING TABLE TO STANDARDS					
T.O.E. Number/Description		Procedures and Controls Required to Comply	IEC61511 Refs. (Clause. Para)	Auditors Comments	Action
1.	General Requirements	Functional Safety Management System	5.2.1	Company does not currently operate an informal FSM based on the 61511 standard.	1. Develop a formal methodology document, based on the existing QMS procedures to capture Company functional safety processes 2. Review the existing QMS procedure against the 61511 lifecycle requirements and develop or modify procedures to ensure all clause are adequately addressed
2.	General Requirements	Functional Safety Policy Statement	5.2.1.1	No formal statement and strategy document in place at the time of the audit	3. Prepare statement to include top level strategy / approach to FS

Typical FS gap analysis record sheet

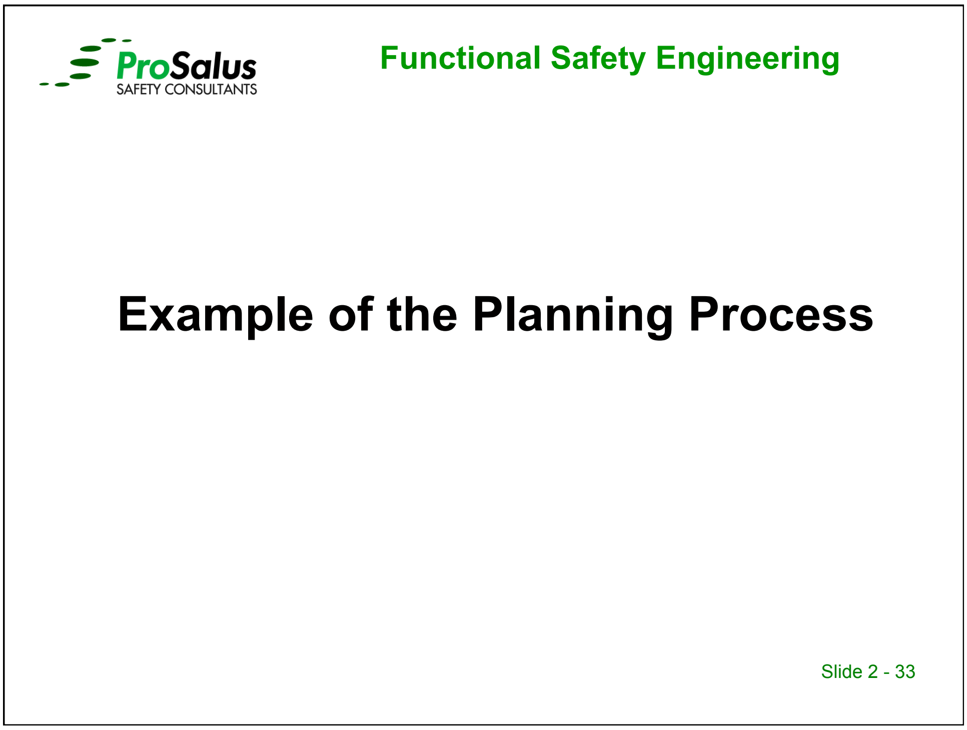
Slide 2 - 31

ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering

- The mapping leads to recommendations to either update, revise or introduce new procedures and work instructions and systems to improve compliance
- Changes to existing systems should be implemented through a:
  - Roll out exercise through out the organisation
  - Series of workshops / toolbox talks to keep staff up to date
- Must include competency testing and assessment of staff that will be directly interfacing with the SIS including operations, maintenance and engineering.

Slide 2 - 32

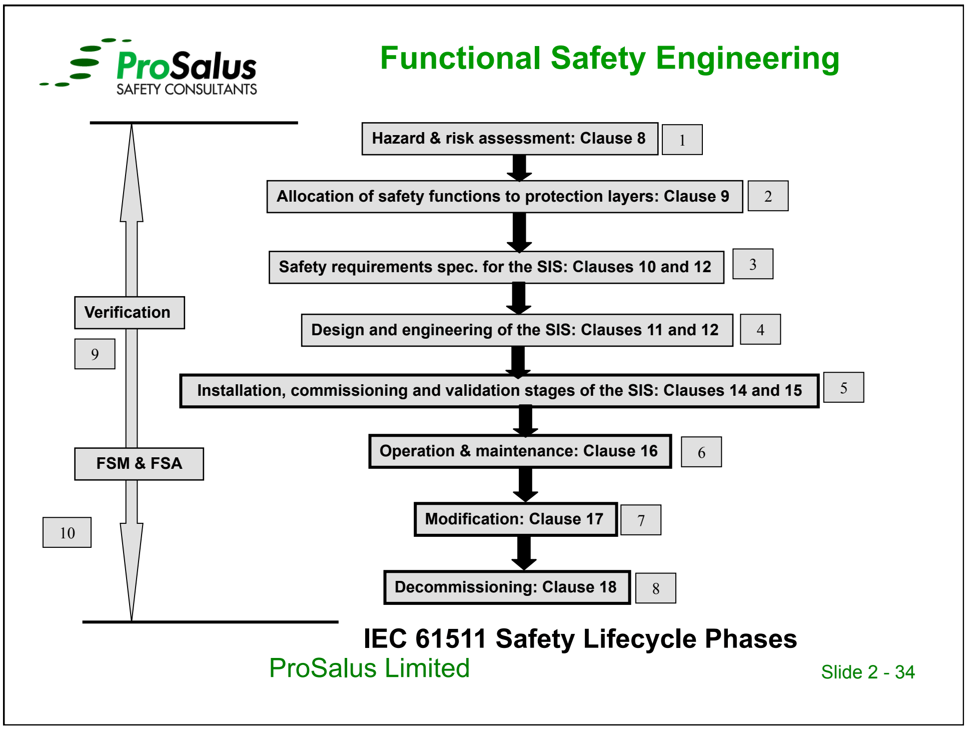


ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of the Planning Process

Slide 2 - 33



ProSalus SAFETY CONSULTANTS

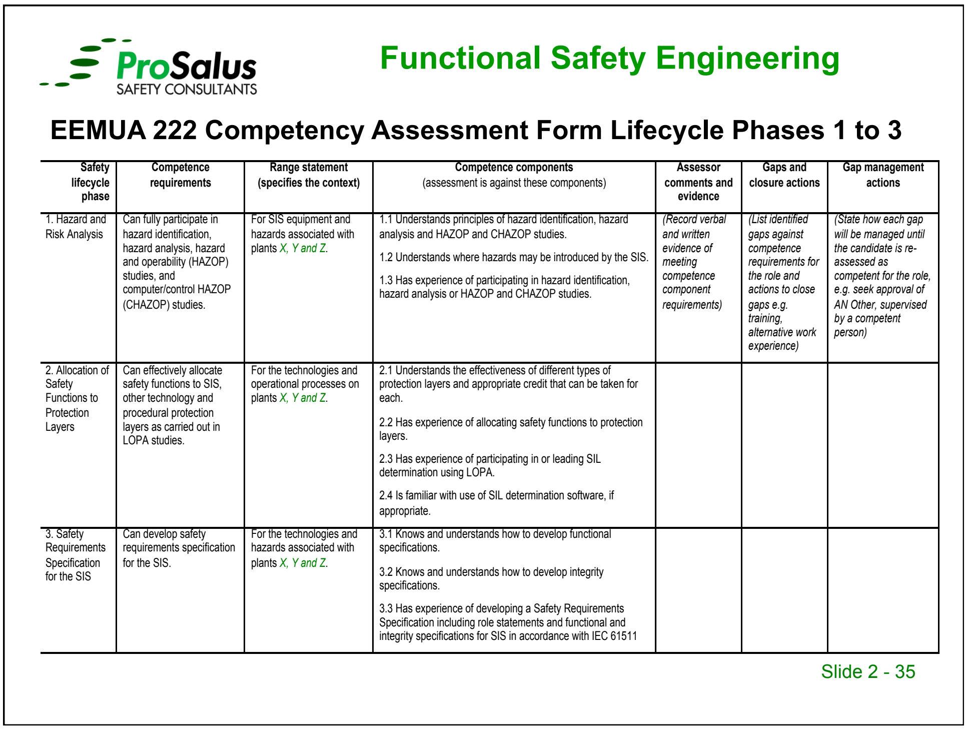
Functional Safety Engineering

Hazard & risk assessment: Clause 8
1
Allocation of safety functions to protection layers: Clause 9
2
Safety requirements spec. for the SIS: Clauses 10 and 12
3
Design and engineering of the SIS: Clauses 11 and 12
4
Installation, commissioning and validation stages of the SIS: Clauses 14 and 15
5
Operation & maintenance: Clause 16
6
Modification: Clause 17
7
Decommissioning: Clause 18
8
Verification
9
FSM & FSA
10

IEC 61511 Safety Lifecycle Phases

ProSalus Limited

Slide 2 - 34



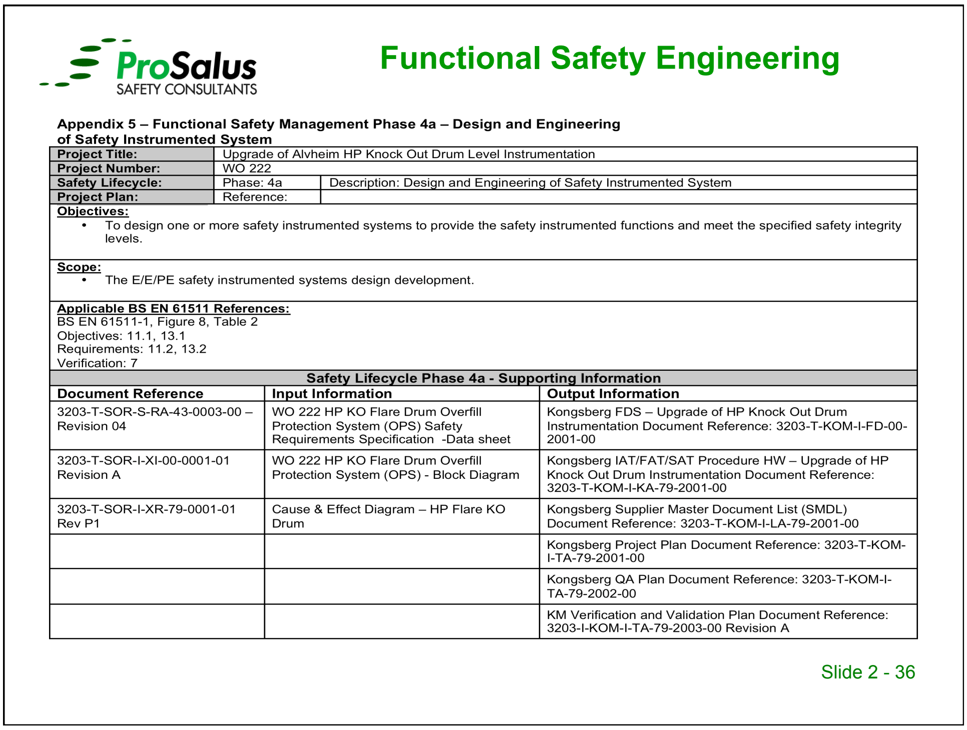
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

EEMUA 222 Competency Assessment Form Lifecycle Phases 1 to 3

Safety lifecycle phase	Competence requirements	Range statement (specifies the context)	Competence components (assessment is against these components)	Assessor comments and evidence	Gaps and closure actions	Gap management actions
1. Hazard and Risk Analysis	Can fully participate in hazard identification, hazard analysis, hazard and operability (HAZOP) studies, and computer/control HAZOP (CHAZOP) studies.	For SIS equipment and hazards associated with plants *X, Y and Z*.	1.1 Understands principles of hazard identification, hazard analysis and HAZOP and CHAZOP studies. 1.2 Understands where hazards may be introduced by the SIS. 1.3 Has experience of participating in hazard identification, hazard analysis or HAZOP and CHAZOP studies.	*(Record verbal and written evidence of meeting competence component requirements)*	*(List identified gaps against competence requirements for the role and actions to close gaps e.g. training, alternative work experience)*	*(State how each gap will be managed until the candidate is re-assessed as competent for the role, e.g. seek approval of AN Other, supervised by a competent person)*
2. Allocation of Safety Functions to Protection Layers	Can effectively allocate safety functions to SIS, other technology and procedural protection layers as carried out in LOPA studies.	For the technologies and operational processes on plants *X, Y and Z*.	2.1 Understands the effectiveness of different types of protection layers and appropriate credit that can be taken for each. 2.2 Has experience of allocating safety functions to protection layers. 2.3 Has experience of participating in or leading SIL determination using LOPA. 2.4 Is familiar with use of SIL determination software, if appropriate.			
3. Safety Requirements Specification for the SIS	Can develop safety requirements specification for the SIS.	For the technologies and hazards associated with plants *X, Y and Z*.	3.1 Knows and understands how to develop functional specifications. 3.2 Knows and understands how to develop integrity specifications. 3.3 Has experience of developing a Safety Requirements Specification including role statements and functional and integrity specifications for SIS in accordance with IEC 61511			

Slide 2 - 35



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Appendix 5 – Functional Safety Management Phase 4a – Design and Engineering of Safety Instrumented System

Project Title:	Upgrade of Alvheim HP Knock Out Drum Level Instrumentation	
Project Number:	WO 222	
Safety Lifecycle:	Phase: 4a	Description: Design and Engineering of Safety Instrumented System
Project Plan:	Reference:	

Objectives:

- To design one or more safety instrumented systems to provide the safety instrumented functions and meet the specified safety integrity levels.

Scope:

- The E/E/PE safety instrumented systems design development.

Applicable BS EN 61511 References:
BS EN 61511-1, Figure 8, Table 2
Objectives: 11.1, 13.1
Requirements: 11.2, 13.2
Verification: 7

Safety Lifecycle Phase 4a - Supporting Information

Document Reference	Input Information	Output Information
3203-T-SOR-S-RA-43-0003-00 – Revision 04	WO 222 HP KO Flare Drum Overfill Protection System (OPS) Safety Requirements Specification -Data sheet	Kongsberg FDS – Upgrade of HP Knock Out Drum Instrumentation Document Reference: 3203-T-KOM-I-FD-00-2001-00
3203-T-SOR-I-XI-00-0001-01 Revision A	WO 222 HP KO Flare Drum Overfill Protection System (OPS) - Block Diagram	Kongsberg IAT/FAT/SAT Procedure HW – Upgrade of HP Knock Out Drum Instrumentation Document Reference: 3203-T-KOM-I-KA-79-2001-00
3203-T-SOR-I-XR-79-0001-01 Rev P1	Cause & Effect Diagram – HP Flare KO Drum	Kongsberg Supplier Master Document List (SMDL) Document Reference: 3203-T-KOM-I-LA-79-2001-00
		Kongsberg Project Plan Document Reference: 3203-T-KOM-I-TA-79-2001-00
		Kongsberg QA Plan Document Reference: 3203-T-KOM-I-TA-79-2002-00
		KM Verification and Validation Plan Document Reference: 3203-I-KOM-I-TA-79-2003-00 Revision A

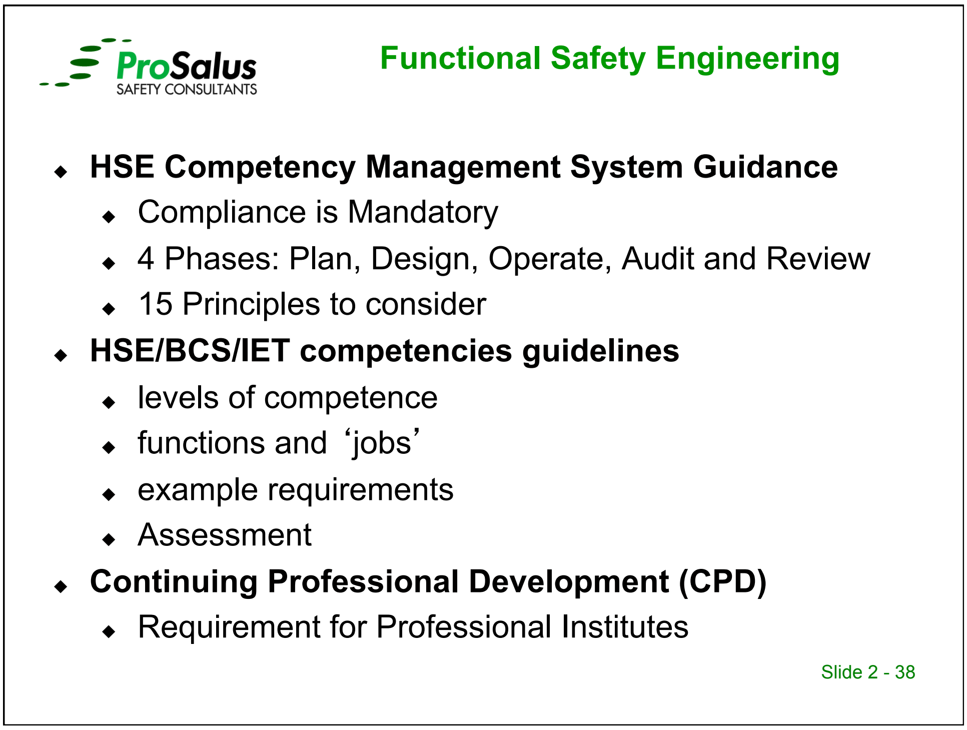
Slide 2 - 36

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Competency Assessment (FSCA)

Slide 2 - 37

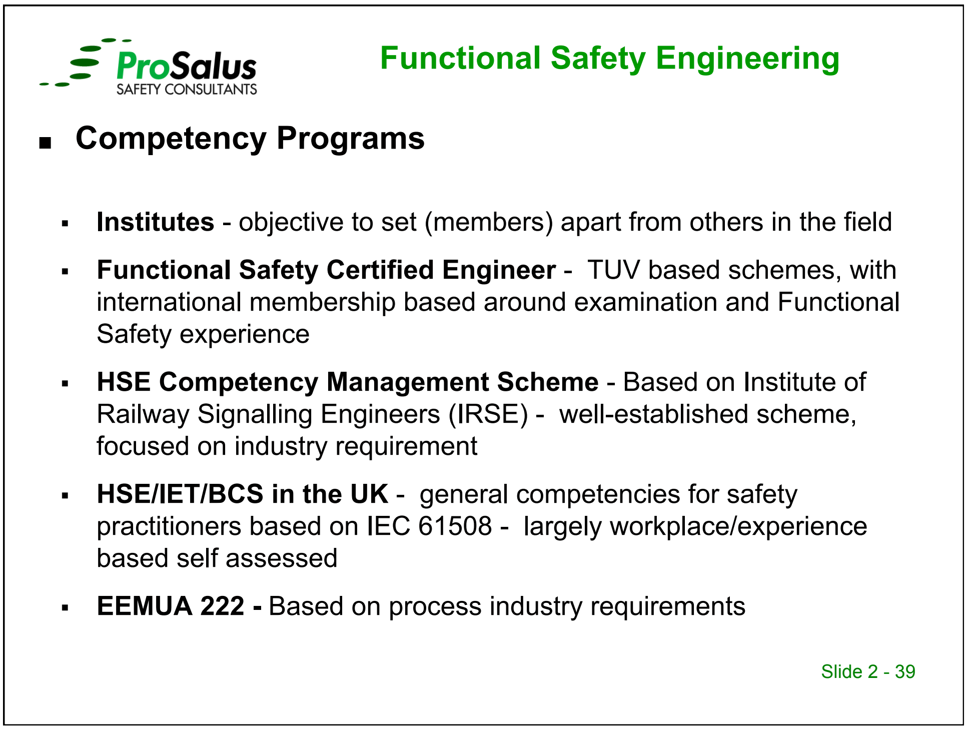


ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **HSE Competency Management System Guidance**
  - Compliance is Mandatory
  - 4 Phases: Plan, Design, Operate, Audit and Review
  - 15 Principles to consider
- **HSE/BCS/IET competencies guidelines**
  - levels of competence
  - functions and ‘jobs’
  - example requirements
  - Assessment
- **Continuing Professional Development (CPD)**
  - Requirement for Professional Institutes

Slide 2 - 38

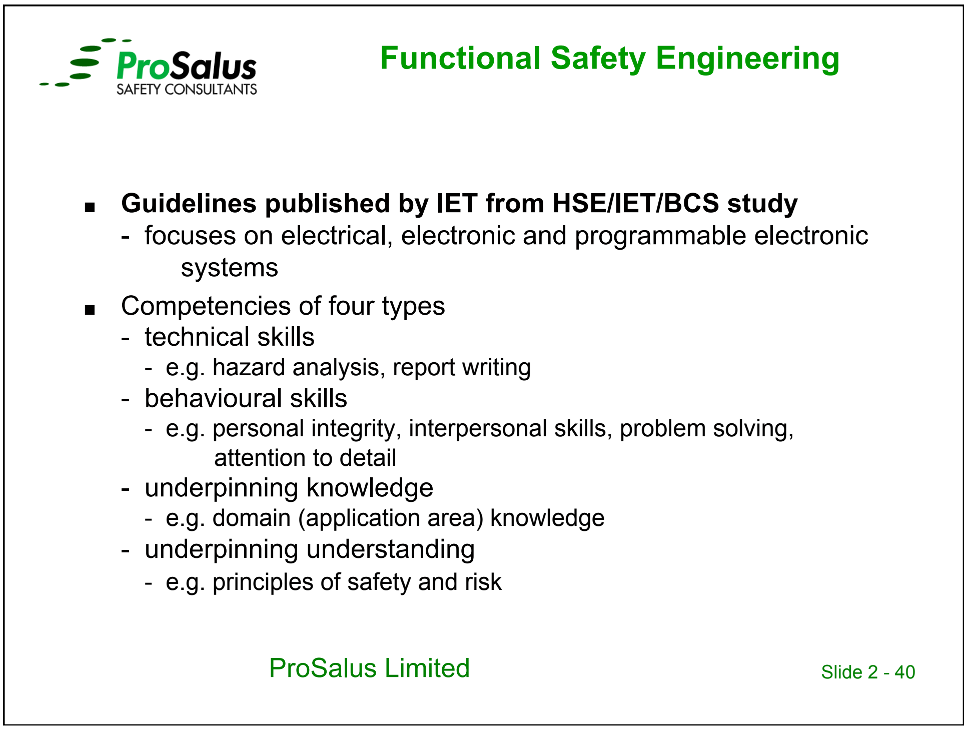


ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Competency Programs**
  - **Institutes** - objective to set (members) apart from others in the field
  - **Functional Safety Certified Engineer** - TUV based schemes, with international membership based around examination and Functional Safety experience
  - **HSE Competency Management Scheme** - Based on Institute of Railway Signalling Engineers (IRSE) - well-established scheme, focused on industry requirement
  - **HSE/IET/BCS in the UK** - general competencies for safety practitioners based on IEC 61508 - largely workplace/experience based self assessed
  - **EEMUA 222 -** Based on process industry requirements

Slide 2 - 39



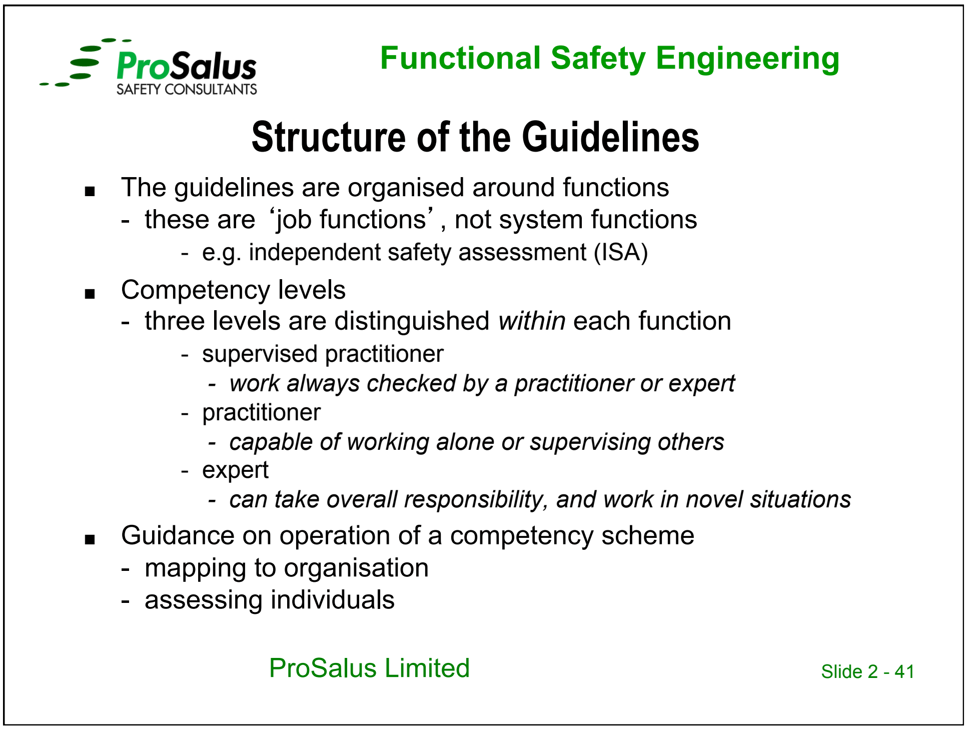
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Guidelines published by IET from HSE/IET/BCS study**
  - focuses on electrical, electronic and programmable electronic systems
- Competencies of four types
  - technical skills
    - e.g. hazard analysis, report writing
  - behavioural skills
    - e.g. personal integrity, interpersonal skills, problem solving, attention to detail
  - underpinning knowledge
    - e.g. domain (application area) knowledge
  - underpinning understanding
    - e.g. principles of safety and risk

ProSalus Limited

Slide 2 - 40



ProSalus SAFETY CONSULTANTS

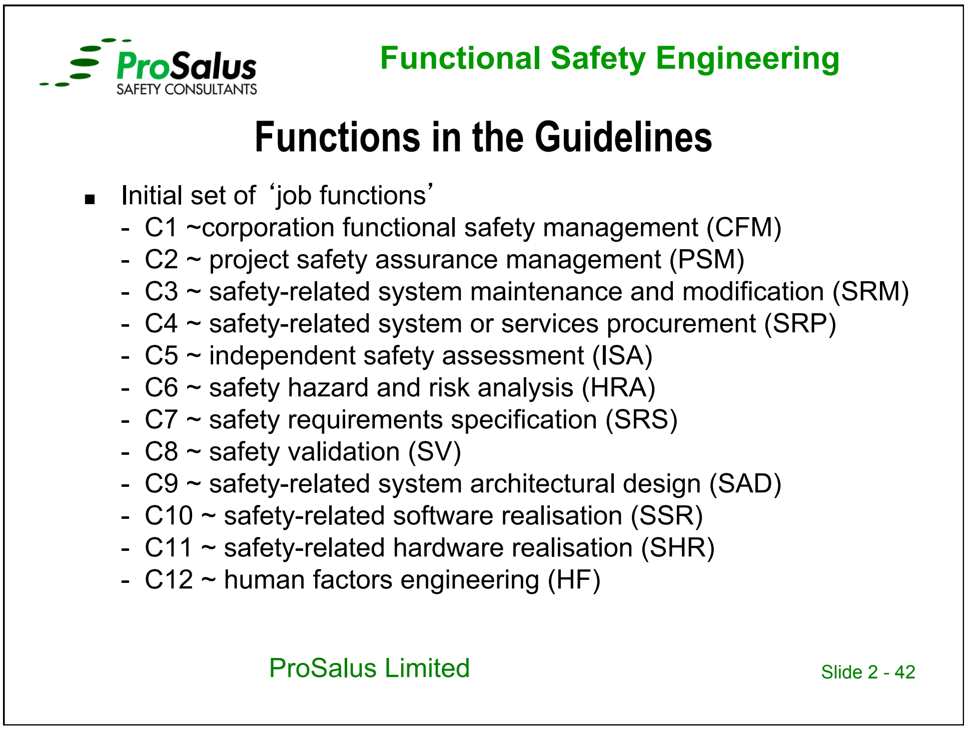
Functional Safety Engineering

Structure of the Guidelines

- The guidelines are organised around functions
  - these are ‘job functions’, not system functions
    - e.g. independent safety assessment (ISA)
- Competency levels
  - three levels are distinguished *within* each function
    - supervised practitioner
      - *work always checked by a practitioner or expert*
    - practitioner
      - *capable of working alone or supervising others*
    - expert
      - *can take overall responsibility, and work in novel situations*
- Guidance on operation of a competency scheme
  - mapping to organisation
  - assessing individuals

ProSalus Limited

Slide 2 - 41



ProSalus SAFETY CONSULTANTS

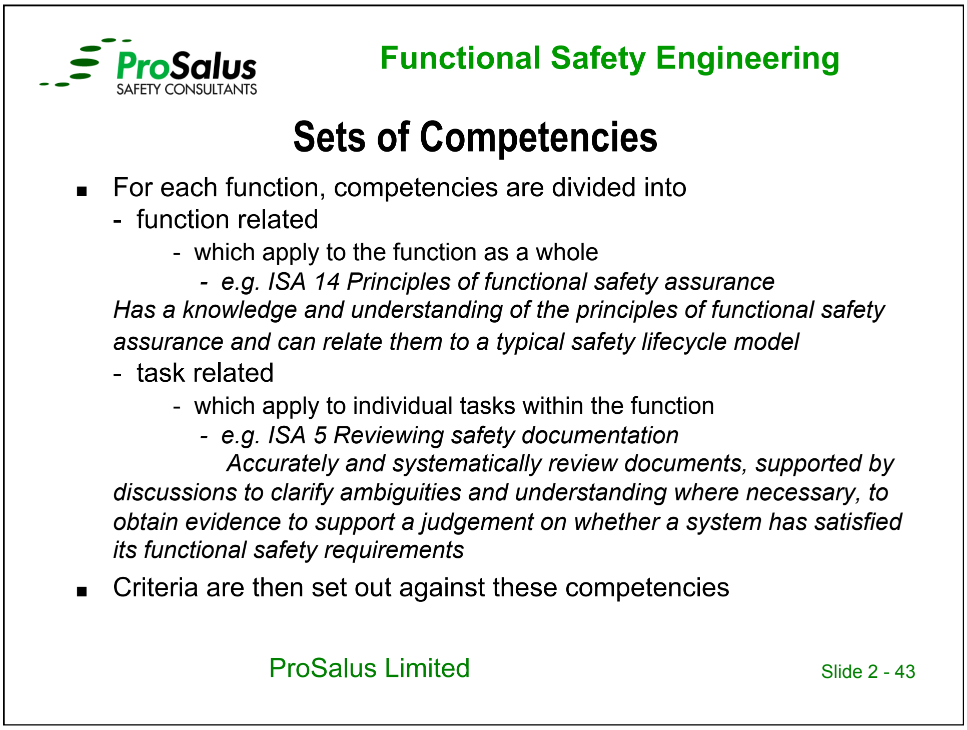
Functional Safety Engineering

Functions in the Guidelines

- Initial set of ‘job functions’
  - C1 ~corporation functional safety management (CFM)
  - C2 ~ project safety assurance management (PSM)
  - C3 ~ safety-related system maintenance and modification (SRM)
  - C4 ~ safety-related system or services procurement (SRP)
  - C5 ~ independent safety assessment (ISA)
  - C6 ~ safety hazard and risk analysis (HRA)
  - C7 ~ safety requirements specification (SRS)
  - C8 ~ safety validation (SV)
  - C9 ~ safety-related system architectural design (SAD)
  - C10 ~ safety-related software realisation (SSR)
  - C11 ~ safety-related hardware realisation (SHR)
  - C12 ~ human factors engineering (HF)

ProSalus Limited

Slide 2 - 42



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Sets of Competencies

- For each function, competencies are divided into
  - function related
    - which apply to the function as a whole
      - *e.g. ISA 14 Principles of functional safety assurance*

Has a knowledge and understanding of the principles of functional safety assurance and can relate them to a typical safety lifecycle model

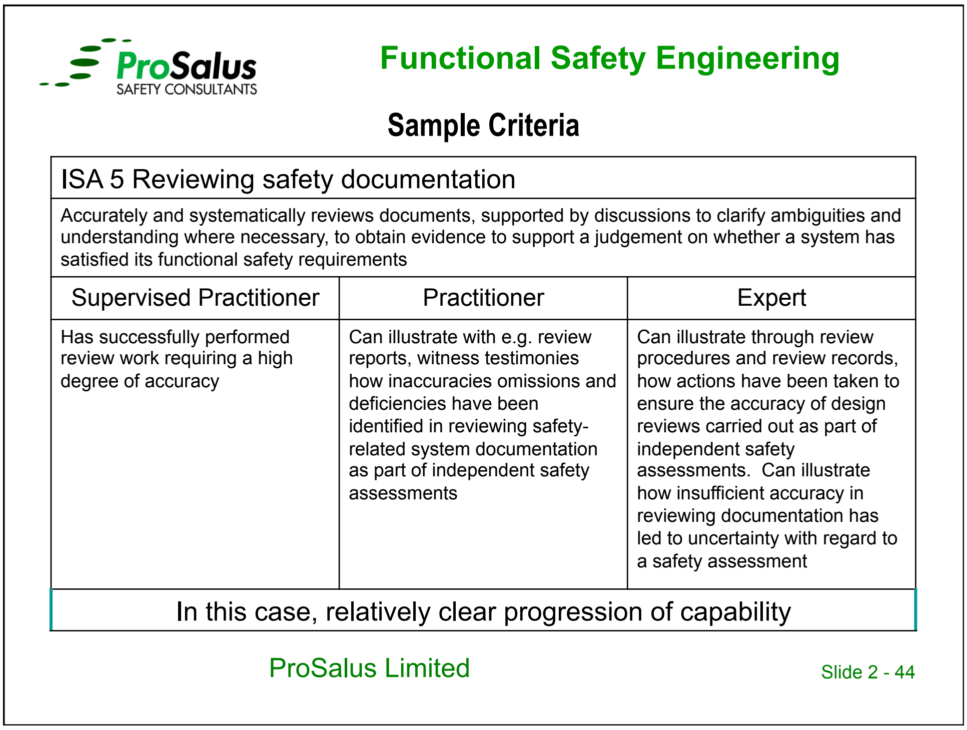
  - task related
    - which apply to individual tasks within the function
      - *e.g. ISA 5 Reviewing safety documentation*

Accurately and systematically review documents, supported by discussions to clarify ambiguities and understanding where necessary, to obtain evidence to support a judgement on whether a system has satisfied its functional safety requirements

- Criteria are then set out against these competencies

ProSalus Limited

Slide 2 - 43



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Sample Criteria

ISA 5 Reviewing safety documentation

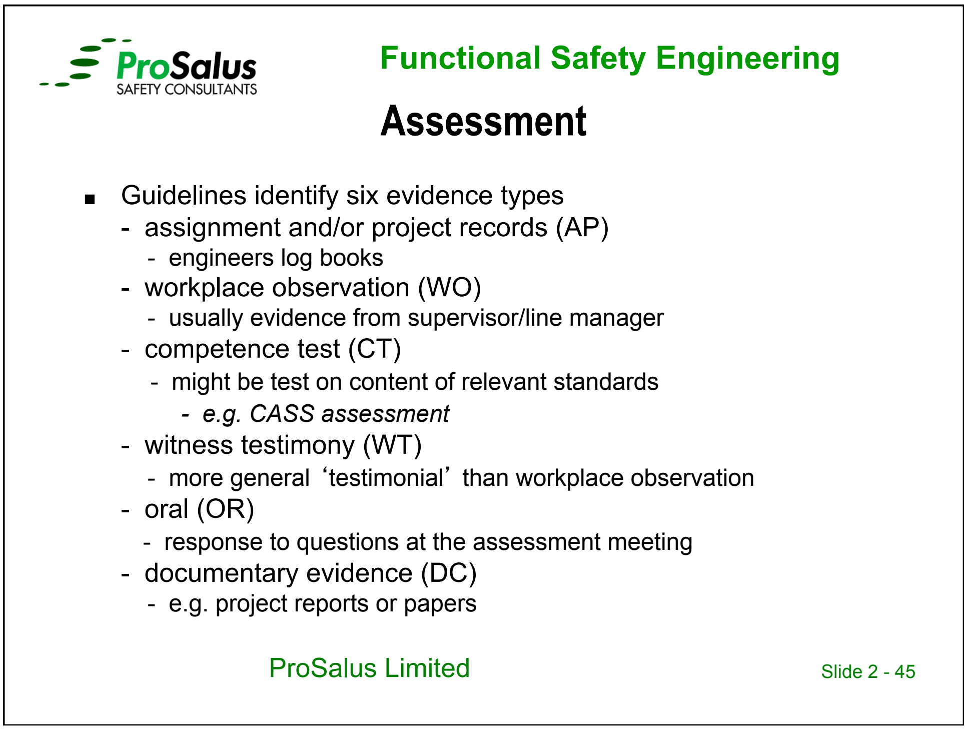
Accurately and systematically reviews documents, supported by discussions to clarify ambiguities and understanding where necessary, to obtain evidence to support a judgement on whether a system has satisfied its functional safety requirements

Supervised Practitioner	Practitioner	Expert
Has successfully performed review work requiring a high degree of accuracy	Can illustrate with e.g. review reports, witness testimonies how inaccuracies omissions and deficiencies have been identified in reviewing safety-related system documentation as part of independent safety assessments	Can illustrate through review procedures and review records, how actions have been taken to ensure the accuracy of design reviews carried out as part of independent safety assessments. Can illustrate how insufficient accuracy in reviewing documentation has led to uncertainty with regard to a safety assessment

In this case, relatively clear progression of capability

ProSalus Limited

Slide 2 - 44



ProSalus SAFETY CONSULTANTS

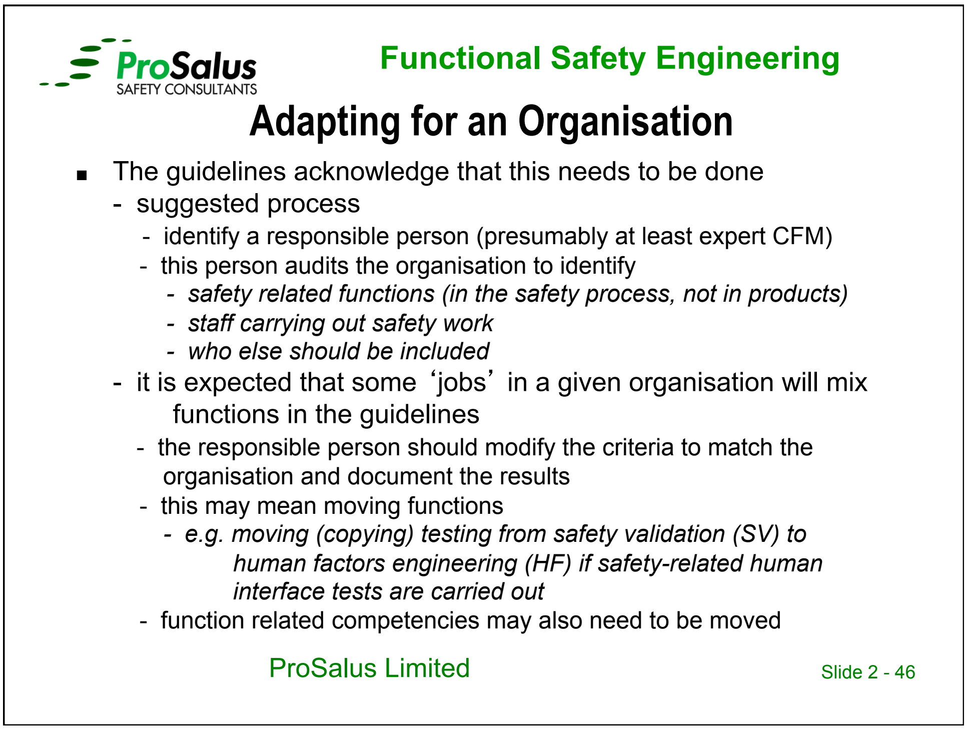
Functional Safety Engineering

Assessment

- Guidelines identify six evidence types
  - assignment and/or project records (AP)
    - engineers log books
  - workplace observation (WO)
    - usually evidence from supervisor/line manager
  - competence test (CT)
    - might be test on content of relevant standards
      - *e.g. CASS assessment*
  - witness testimony (WT)
    - more general ‘testimonial’ than workplace observation
  - oral (OR)
    - response to questions at the assessment meeting
  - documentary evidence (DC)
    - e.g. project reports or papers

ProSalus Limited

Slide 2 - 45



ProSalus SAFETY CONSULTANTS

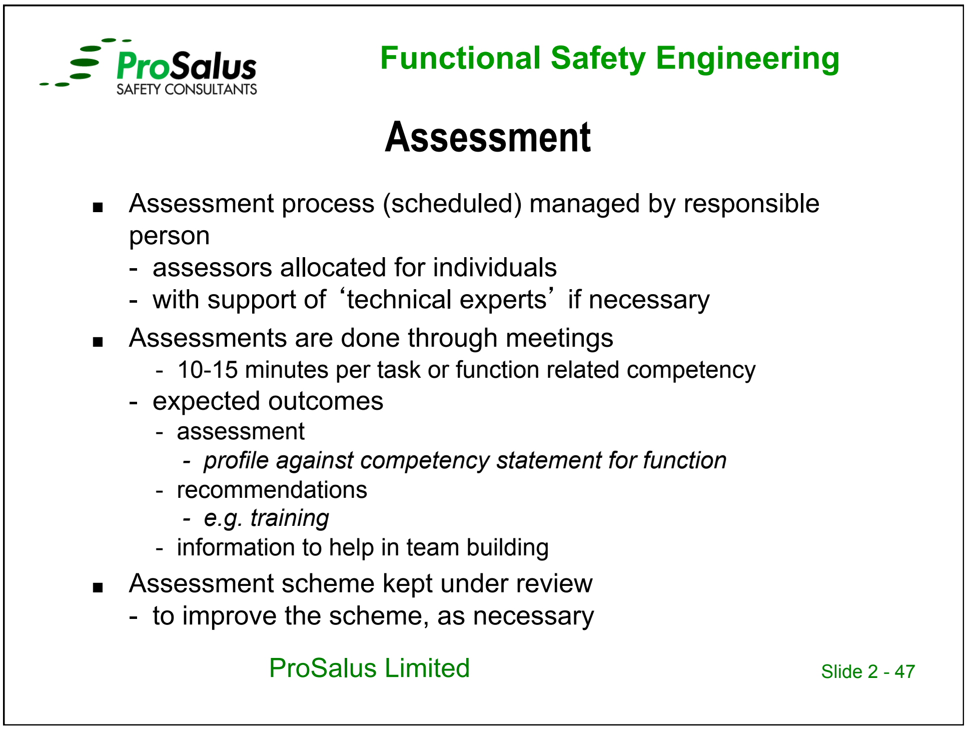
Functional Safety Engineering

Adapting for an Organisation

- The guidelines acknowledge that this needs to be done
  - suggested process
    - identify a responsible person (presumably at least expert CFM)
    - this person audits the organisation to identify
      - *safety related functions (in the safety process, not in products)*
      - *staff carrying out safety work*
      - *who else should be included*
  - it is expected that some ‘jobs’ in a given organisation will mix functions in the guidelines
    - the responsible person should modify the criteria to match the organisation and document the results
    - this may mean moving functions
      - *e.g. moving (copying) testing from safety validation (SV) to human factors engineering (HF) if safety-related human interface tests are carried out*
    - function related competencies may also need to be moved

ProSalus Limited

Slide 2 - 46



ProSalus
SAFETY CONSULTANTS

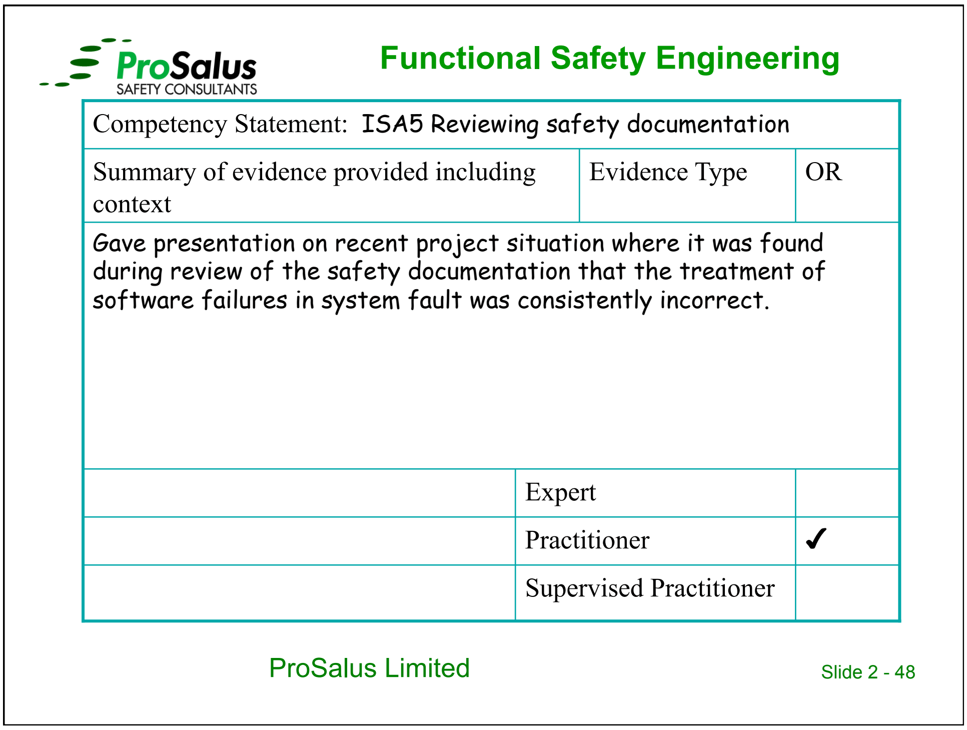
Functional Safety Engineering

Assessment

- Assessment process (scheduled) managed by responsible person
  - assessors allocated for individuals
  - with support of 'technical experts' if necessary
- Assessments are done through meetings
  - 10-15 minutes per task or function related competency
  - expected outcomes
    - assessment
      - *profile against competency statement for function*
    - recommendations
      - *e.g. training*
    - information to help in team building
- Assessment scheme kept under review
  - to improve the scheme, as necessary

ProSalus Limited

Slide 2 - 47



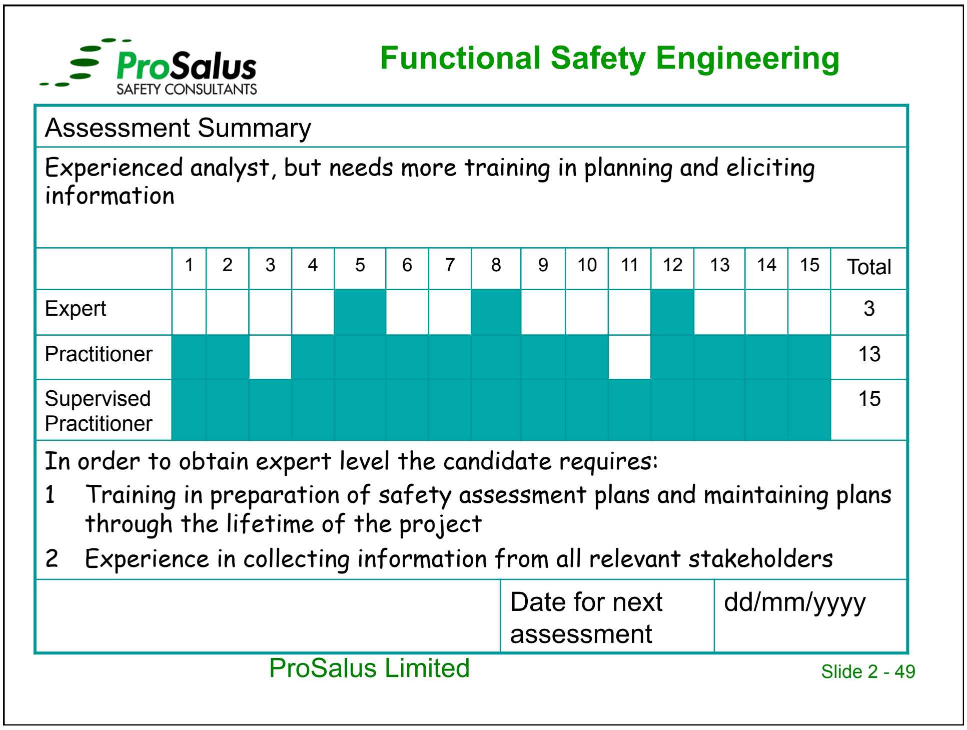
ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering

Competency Statement: ISA5 Reviewing safety documentation		
Summary of evidence provided including context	Evidence Type	OR
Gave presentation on recent project situation where it was found during review of the safety documentation that the treatment of software failures in system fault was consistently incorrect.		
	Expert	
	Practitioner	✓
	Supervised Practitioner	

ProSalus Limited

Slide 2 - 48



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Assessment Summary

Experienced analyst, but needs more training in planning and eliciting information

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Total
Expert					■			■				■				3
Practitioner	■	■		■	■	■	■	■	■	■		■	■	■	■	13
Supervised Practitioner	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	15

In order to obtain expert level the candidate requires:

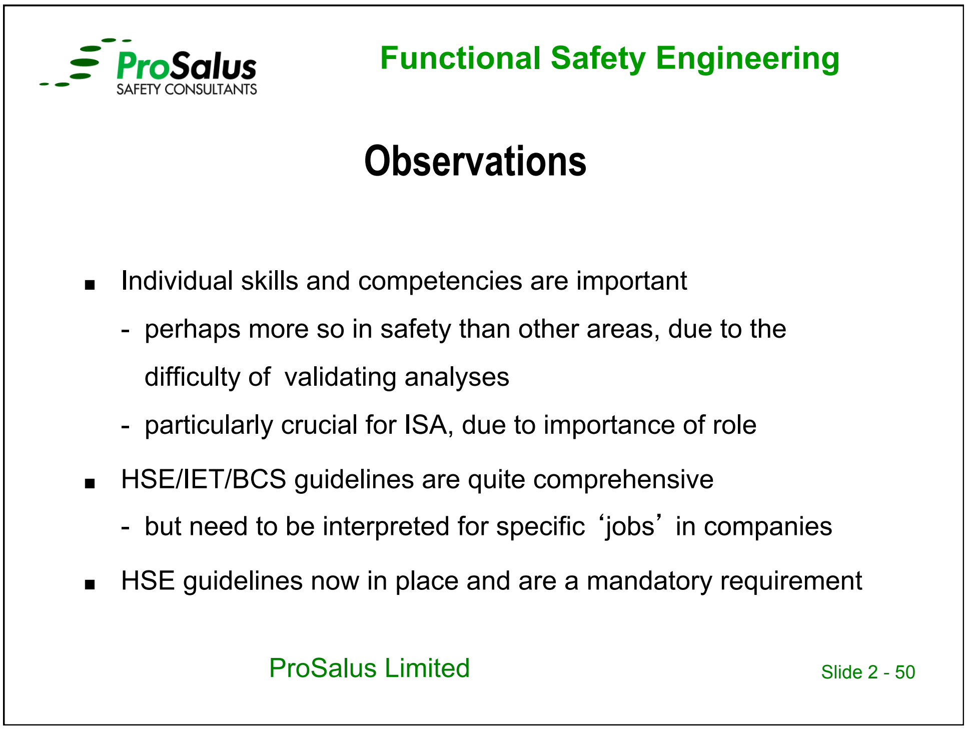
1 Training in preparation of safety assessment plans and maintaining plans through the lifetime of the project

2 Experience in collecting information from all relevant stakeholders

	Date for next assessment	dd/mm/yyyy

ProSalus Limited

Slide 2 - 49



ProSalus SAFETY CONSULTANTS

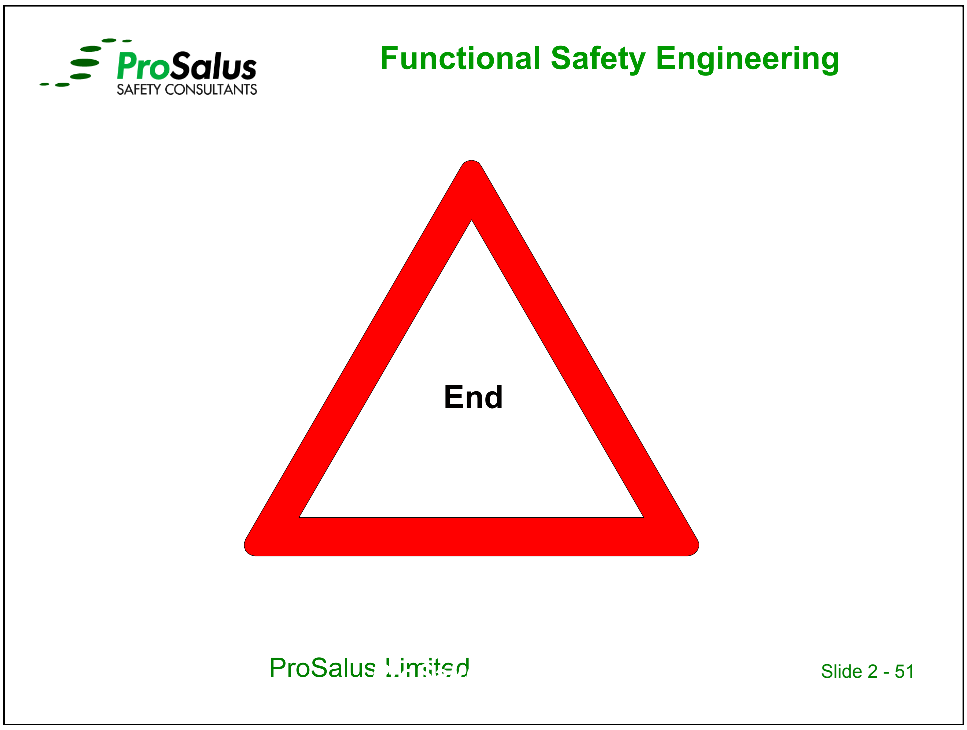
Functional Safety Engineering

Observations

- Individual skills and competencies are important
  - perhaps more so in safety than other areas, due to the difficulty of validating analyses
  - particularly crucial for ISA, due to importance of role
- HSE/IET/BCS guidelines are quite comprehensive
  - but need to be interpreted for specific ‘jobs’ in companies
- HSE guidelines now in place and are a mandatory requirement

ProSalus Limited

Slide 2 - 50



ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

End

ProSalus Limited

Slide 2 - 51